IBM Security Identity Manager
Version 6.0

UNIX and Linux Adapter Installation and Configuration Guide
Contents

Figures ........................................ v

Tables ........................................ vii

Preface ........................................ ix
About this publication ........................ ix
Access to publications and terminology .... ix
Accessibility ..................................... x
Technical training ................................ x
Support information ............................. x
Statement of Good Security Practices ....... x

Chapter 1. UNIX and Linux Adapter
Installation and Configuration Guide . . 1
Overview of the adapter ....................... 1
Features of the adapter ....................... 1
Architecture of the adapter ................... 1
Supported configurations .................... 2

Chapter 2. Adapter installation planning 5
Preinstallation roadmap ....................... 5
Installation roadmap .......................... 5
Prerequisites .................................. 6
Installation worksheet for the adapter ...... 8
Software download ............................ 8

Chapter 3. Adapter installation 9
Dispatcher installation verification ......... 9
Installing the UNIX and Linux Adapter .... 9
Installation verification ....................... 10
Adapter service start, stop, and restart .... 11
Importing the adapter profile into the IBM Security
Identity Manager server ....................... 11
Adapter profile installation verification ... 12
Communicating with the Secure Shell protocol 12
Adapter user account creation ............... 13
Creating a service ............................ 14

Chapter 4. Adapter installation and
uninstallation in silent mode ............... 21
Installing the adapter in silent mode ....... 21
Uninstalling the adapter in silent mode ........ 22

Chapter 5. First steps after installation 23
Adapter configuration ........................ 23
Customizing the adapter profile ............. 23
Running user-defined scripts ................. 25
Defining the maximum connection count for
adapter operations ........................... 26
User home directory creation ................. 28
Editing adapter profiles on the UNIX or Linux
operating system ............................. 28
Adapter features customization and extension 28
Optional feature configuration .............. 29
Customizing password prompt attributes .... 29
Adding home directory permissions on the
account form ................................. 30
Adding umask settings on the account form .... 31
Setting up locales ............................ 32
Configuring alternative adapter scripts location 32
Reconciling with custom scripts ............. 33
Ending a user session after suspension ....... 34
Ending user processes to delete a user account 34
Configuring last access date support for Solaris systems ........ 35
Non-login account (passwd-n) support .... 36
Password management for account restoration ... 38
Language pack installation .................. 39
Verifying that the adapter is working correctly 39

Chapter 6. Adapter error
troubleshooting .............................. 41
Techniques for troubleshooting problems ... 41
Warning and error messages ................. 43
Solving adapter installation and operational
problems ...................................... 46
Known adapter issues ........................ 48
/tmp directory permissions .................. 48
Home directory permissions ................. 48
HP-UX password age issues ................. 48
No support for adding the primary group of a
user to the secondary groupset of the user 49

Chapter 7. Adapter upgrade ............... 51
Connector upgrade ........................... 51
Dispatcher upgrade ........................... 51
Upgrade of an existing adapter profile ....... 51

Chapter 8. Adapter uninstallation ....... 53
Uninstalling the adapter from the Tivoli Directory Integrator server ........ 53
Adapter profile removal from the IBM Security Identity Manager server ........ 53

Chapter 9. Adapter reinstallation ....... 55
Appendix A. Adapter attributes ......... 57
Group form attributes ....................... 66
Attributes by UNIX and Linux Adapter actions ........ 66
System Login Add .......................... 67
System Login Change ....................... 67
System Login Delete ......................... 67
System Login Suspend ....................... 67
System Login Restore ....................... 68
Test ........................................ 68
Reconciliation ............................... 68
Group add .................................. 69
Figures

1. The architecture of the UNIX and Linux Adapter ... 2
2. Example of a single server configuration ... 2
3. Example of multiple server configuration ... 3
Tables

1. Preinstallation roadmap ........................................................... 5
2. Installation roadmap ............................................................... 5
3. Prerequisites to install the adapter ........................................... 6
4. Required information to install the adapter ............................... 8
5. Adapter components ............................................................... 10
6. Secure Shell configuration ...................................................... 13
7. silent mode parameters for installing ....................................... 21
8. silent mode parameter for uninstalling ..................................... 22
9. No Password Account possible outcomes ................................. 37
10. Warning and error messages .................................................... 43
11. Search strings for software versions ....................................... 46
12. Reconciliation file names ....................................................... 47
13. Account form attributes, descriptions, permissions, and applicable operating systems ................................. 57
14. Group form attributes ............................................................ 66
15. Add request attributes for AIX, HPUX, Linux, and Solaris ............ 67
16. Change request attributes for AIX, HPUX, Linux, and Solaris ........... 67
17. Delete request attributes for AIX and Solaris ............................ 67
18. Delete request attributes for HPUX and Linux .......................... 67
19. Suspend request attributes for AIX and Solaris .......................... 67
20. Suspend request attributes for HP-UX and Linux ......................... 67
21. Restore request attributes for AIX ........................................... 68
22. Restore request attributes for Solaris ....................................... 68
23. Test attributes ........................................................................ 68
24. Reconciliation request attributes for AIX and Solaris .................. 68
25. Reconciliation request attributes for HP-UX and Linux ............... 68
26. Group add request attribute for AIX, HPUX, Linux, and Solaris ....... 69
27. Group change request attribute for AIX, HPUX, Linux, and Solaris .. 69
28. Sudo access command and file setup ....................................... 79
Preface

About this publication

The UNIX and Linux Adapter Installation and Configuration Guide provides the basic information that you use to install and configure the IBM® Security Identity Manager UNIX and Linux Adapter. The UNIX and Linux Adapter enables connectivity between the IBM Security Identity Manager server and a system that runs a UNIX or Linux operating system.

Access to publications and terminology

This section provides:
- A list of publications in the IBM Security Identity Manager library.
- Links to Online publications.
- A link to the IBM Terminology website.

IBM Security Identity Manager library


Online publications

IBM posts product publications when the product is released and when the publications are updated at the following locations:

IBM Security Identity Manager library


IBM Security Systems Documentation Central

[IBM Security Systems Documentation Central](http://www-01.ibm.com/support/knowledgecenter/SSRMWJ/welcome) provides an alphabetical list of all IBM Security Systems product libraries and links to the online documentation for specific versions of each product.

IBM Publications Center


IBM Terminology website

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

Technical training

For technical training information, see the following IBM Education website at [http://www.ibm.com/software/tivoli/education](http://www.ibm.com/software/tivoli/education).

Support information

IBM Support provides assistance with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at [http://www.ibm.com/software/support/probsub.html](http://www.ibm.com/software/support/probsub.html).

Appendix F, “Support information,” on page 99 provides details about:

- What information to collect before contacting IBM Support.
- The various methods for contacting IBM Support.
- How to use IBM Support Assistant.
- Instructions and problem-determination resources to isolate and fix the problem yourself.

Note: The Community and Support tab on the product information center can provide additional support resources.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.
Chapter 1. UNIX and Linux Adapter Installation and Configuration Guide

This installation guide provides the basic information to install and configure the UNIX and Linux Adapter. The adapter enables connectivity between the IBM Security Identity Manager server and the managed resource.

Overview of the adapter

An adapter provides an interface between a managed resource and the IBM Security Identity Manager server.

Adapters might reside on the managed resource. The IBM Security Identity Manager server manages access to the resource by using your security system. Adapters function as trusted virtual administrators on the target platform. They do tasks, such as creating, suspending, and restoring user accounts, and other administrative functions that are done manually. The adapter runs as a service, independently of whether you are logged on to the IBM Security Identity Manager server.

The UNIX and Linux Adapter enables communication between the IBM Security Identity Manager server and any of the following operating systems:
- AIX®
- HPUX
- Linux
- Solaris

Features of the adapter

The adapter automates the various user account administrative tasks.

The adapter automates the following user management tasks:
- Adding user accounts
- Modifying user account attributes
- Modifying user account passwords
- Suspending, restoring, and deleting user accounts
- Managing groups
- Reconciling user accounts and groups

Architecture of the adapter

You must install various components for the adapter to function correctly.

You install the following components:
- The Dispatcher
- The IBM Tivoli® Directory Integrator connector
- The IBM Security Identity Manager adapter profile
You must install the Dispatcher and the adapter profile; however, the Tivoli Directory Integrator connector might already be installed with the base Tivoli Directory Integrator product.

Figure 1 describes the components that work together to complete the user account management tasks in a Tivoli Directory Integrator environment.

Figure 1. The architecture of the UNIX and Linux Adapter

For more information about Tivoli Directory Integrator, see the Quick Start Guide in the IBM Security Identity Manager product documentation.

Supported configurations

The adapter supports both single server and multiple server configurations.

There are fundamental components in each environment.

- The IBM Security Identity Manager server
- The IBM Tivoli Directory Integrator server
- The managed resource
- The adapter

The adapter must be directly on the server that runs the Tivoli Directory Integrator server.

Single server configuration

Install the IBM Security Identity Manager server, the Tivoli Directory Integrator server, and the UNIX and Linux Adapter on one server to establish communication with the UNIX or Linux operating system. Install the UNIX or Linux operating system on a different server as described.

Figure 2

Multiple server configuration

Install the IBM Security Identity Manager server, the Tivoli Directory Integrator server, the UNIX and Linux Adapter, and the UNIX or Linux operating system on different servers. Install the Tivoli Directory Integrator server...
server and the UNIX and Linux Adapter on the same server as described

Figure 3

Figure 3. Example of multiple server configuration
Chapter 2. Adapter installation planning

Installing and configuring the adapter involves several steps that you must complete in an appropriate sequence. Review the roadmaps before you begin the installation process.

Preinstallation roadmap

Before you install the adapter, prepare the environment.

Do the tasks that are listed in Table 1.

**Table 1. Preinstallation roadmap**

<table>
<thead>
<tr>
<th>Task</th>
<th>For more information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain the installation software.</td>
<td>Download the software from Passport Advantage® website. See “Software download” on page 8.</td>
</tr>
<tr>
<td>Verify that your environment meets the software and hardware requirements for the adapter.</td>
<td>See “Prerequisites” on page 6.</td>
</tr>
<tr>
<td>Obtain and install the Dispatcher.</td>
<td>Download the software from Passport Advantage® website. See “Software download” on page 8. Follow the installation instructions in the dispatcher download package.</td>
</tr>
<tr>
<td>Obtain the necessary information for the installation and configuration.</td>
<td>See “Installation worksheet for the adapter” on page 8.</td>
</tr>
</tbody>
</table>

Installation roadmap

Installation of the adapter requires several sequential tasks. Use this roadmap navigate through the installation process.

To install the adapter, complete the tasks that are listed in Table 2.

**Table 2. Installation roadmap**

<table>
<thead>
<tr>
<th>Task</th>
<th>For more information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install the adapter.</td>
<td>See “Installing the UNIX and Linux Adapter” on page 9</td>
</tr>
<tr>
<td>Verify the installation.</td>
<td>See “Installation verification” on page 10</td>
</tr>
<tr>
<td>Import the adapter profile.</td>
<td>See “Importing the adapter profile into the IBM Security Identity Manager server” on page 11</td>
</tr>
<tr>
<td>Verify the profile installation.</td>
<td>See “Adapter profile installation verification” on page 12</td>
</tr>
<tr>
<td>Install the Secure Shell protocol.</td>
<td>See “Communicating with the Secure Shell protocol” on page 12</td>
</tr>
<tr>
<td>Create an adapter user account.</td>
<td>See “Adapter user account creation” on page 13</td>
</tr>
</tbody>
</table>
Table 2. Installation roadmap (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>For more information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a service.</td>
<td>See “Creating a service” on page 14.</td>
</tr>
<tr>
<td>Configure the adapter.</td>
<td>See “Adapter configuration” on page 23.</td>
</tr>
</tbody>
</table>

Prerequisites

Verify that your environment meets all the prerequisites before you install the adapter.

This adapter is installed into IBM Tivoli Directory Integrator. The adapter can be installed on any operating system that is supported by Tivoli Directory Integrator and supported by the target system libraries or client.

Install Tivoli Directory Integrator on each node of the IBM Security Identity Manager WebSphere® Application Server cluster. Then, install this adapter on each instance of Tivoli Directory Integrator.

Table 3 identifies the software and operating system prerequisites for the adapter installation.

See the Release Notes bundled with this adapter package for the most current information about supported versions and minimum fix pack levels.

Table 3. Prerequisites to install the adapter

<table>
<thead>
<tr>
<th>Prerequisite</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tivoli Directory Integrator server</td>
<td>Version 7.1 fix pack 5 or later</td>
</tr>
<tr>
<td></td>
<td>Version 7.1.1 with fix pack 1 and Interim Fix 7.1.1-TIV-TDI-LA0001 or higher</td>
</tr>
<tr>
<td>IBM Security Identity Manager server</td>
<td>Version 6.0</td>
</tr>
<tr>
<td>Prerequisite</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Operating systems</td>
<td>Use the UNIX and Linux Adapter for user provisioning on the following</td>
</tr>
<tr>
<td></td>
<td>operating systems.</td>
</tr>
<tr>
<td></td>
<td><strong>AIX</strong></td>
</tr>
<tr>
<td></td>
<td>AIX 6.1</td>
</tr>
<tr>
<td></td>
<td>AIX 7.1</td>
</tr>
<tr>
<td></td>
<td><strong>HP-UX</strong></td>
</tr>
<tr>
<td></td>
<td>HP-UX 11i</td>
</tr>
<tr>
<td></td>
<td>HP-UX 11i v2</td>
</tr>
<tr>
<td></td>
<td>HP-UX 11i v3</td>
</tr>
<tr>
<td></td>
<td>Supported operating system modes: non-trusted, trusted, and non-secure</td>
</tr>
<tr>
<td></td>
<td><strong>Oracle Solaris</strong></td>
</tr>
<tr>
<td></td>
<td>Solaris 10</td>
</tr>
<tr>
<td></td>
<td>Solaris 11</td>
</tr>
<tr>
<td></td>
<td><strong>Oracle Linux</strong></td>
</tr>
<tr>
<td></td>
<td>Linux 6.3</td>
</tr>
<tr>
<td></td>
<td><strong>Red Hat Linux</strong></td>
</tr>
<tr>
<td></td>
<td>Red Hat Linux Enterprise Server 5.9</td>
</tr>
<tr>
<td></td>
<td>Red Hat Linux Enterprise Server 6.3</td>
</tr>
<tr>
<td></td>
<td>Red Hat Linux Advanced Server 5.9</td>
</tr>
<tr>
<td></td>
<td>Red Hat Linux Advanced Server 6.3</td>
</tr>
<tr>
<td></td>
<td><strong>SuSE Enterprise Linux Server</strong></td>
</tr>
<tr>
<td></td>
<td>SuSE SLES 10</td>
</tr>
<tr>
<td></td>
<td>SuSE SLES 11</td>
</tr>
<tr>
<td></td>
<td>SuSE SLES 11 on zSeries</td>
</tr>
<tr>
<td>System Administrator Authority</td>
<td>To complete the adapter installation procedure, you must have system</td>
</tr>
<tr>
<td></td>
<td>administrator authority.</td>
</tr>
<tr>
<td>Tivoli Directory Integrator adapters</td>
<td>A Tivoli Directory Integrator adapters solution directory is a Tivoli</td>
</tr>
<tr>
<td>solution directory</td>
<td>Directory Integrator work directory for IBM Security Identity Manager</td>
</tr>
<tr>
<td></td>
<td>adapters. See the <em>Dispatcher Installation and Configuration Guide</em>.</td>
</tr>
<tr>
<td>The <code>/etc/passwd</code> and</td>
<td>The <code>/etc/passwd</code> and <code>/etc/shadow/passwd</code> files must be in a standard</td>
</tr>
<tr>
<td><code>/etc/shadow/passwd</code> files in a</td>
<td>format on the managed resource. Any non-standard deviation in these files,</td>
</tr>
<tr>
<td>standard format on the managed</td>
<td>such as more fields or characters, might cause adapter operations to fail.</td>
</tr>
<tr>
<td>resource</td>
<td>The Secure Shell (SSH) protocol</td>
</tr>
<tr>
<td></td>
<td>The Secure Shell (SSH) protocol must be installed and running on the</td>
</tr>
<tr>
<td></td>
<td>managed resource.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The adapter supports OpenSSH and Tectia SSH package.</td>
</tr>
</tbody>
</table>

For information about the prerequisites and supported operating systems for Tivoli Directory Integrator, see the applicable *IBM Tivoli Directory Integrator Administrator Guide*. 

---

Chapter 2. Adapter installation planning 7
Installation worksheet for the adapter

Use this information before you install the adapter.

Table 4. Required information to install the adapter

<table>
<thead>
<tr>
<th>Required information</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tivoli Directory Integrator Home Directory</td>
<td>The ITDI_HOME directory contains the jars/connectors subdirectory. This subdirectory contains adapter JAR files.</td>
<td>IBM Tivoli Directory Integrator can be automatically installed with your IBM Security Identity Manager product. In this case, one of the following is the default directory path that is used for Tivoli Directory Integrator.</td>
</tr>
<tr>
<td>Windows:</td>
<td>drive:\Program Files\IBM\TDI\TDI_VERSION</td>
<td>Windows: drive:\Program Files\IBM\TDI\TDI_VERSION</td>
</tr>
<tr>
<td>UNIX:</td>
<td>/opt/IBM/TDI/TDI_VERSION</td>
<td>UNIX: /opt/IBM/TDI/TDI_VERSION</td>
</tr>
<tr>
<td>Adapters solution directory</td>
<td>When you install the dispatcher, the adapter prompts you to specify a file path for the adapter solution directory. If you do not specify a directory, the default directory is timsol.</td>
<td>Windows: drive:\Program Files\IBM\TDI\TDI_VERSION\Timsol</td>
</tr>
<tr>
<td>Windows:</td>
<td>drive:\Program Files\IBM\TDI\TDI_VERSION\Timsol</td>
<td>UNIX: /opt/IBM/TDI/TDI_VERSION\Timsol</td>
</tr>
</tbody>
</table>

Software download

Download the software through your account at the IBM Passport Advantage website.

Go to IBM Passport Advantage

See the IBM Security Identity Manager Download Document for instructions.

Note:

You can also obtain additional adapter information from IBM Support.
Chapter 3. Adapter installation

All the adapters that are based on Tivoli Directory Integrator require the Dispatcher for the adapters to function correctly.

If the Dispatcher is installed from a previous installation, do not reinstall it unless there is an upgrade to the Dispatcher. See the Dispatcher Installation and Configuration Guide.

After verifying the Dispatcher installation, you might need to install the Tivoli Directory Integrator connector. Depending on your adapter, the connector might already be installed as part of the Tivoli Directory Integrator product and no further action is required.

**Dispatcher installation verification**

If this installation is the first adapter installation that is based on Tivoli Directory Integrator, you must install the Dispatcher before you install the adapter.

Install the Dispatcher on the same Tivoli Directory Integrator server where you want to install the adapter.

Obtain the dispatcher installer from the IBM Passport Advantage website. For information about Dispatcher installation, see the Dispatcher Installation and Configuration Guide.

**Installing the UNIX and Linux Adapter**

Use these steps to install the UNIX and Linux Adapter software.

**Before you begin**

Make sure that you do the following actions:

- See the Release Notes bundled with this adapter package for any updates on installation and configuration steps.
- Verify that your site meets all the prerequisite requirements. See “Prerequisites” on page 6.
- Verify that the Dispatcher is installed before you install the UNIX and Linux Adapter. See “Software download” on page 8. Follow the installation instructions included in the dispatcher download package.
- Obtain a copy of the installation software. See “Software download” on page 8.
- Obtain system administrator authority. See “Prerequisites” on page 6.

**About this task**

Use the PosixAdapterInstall_70.jar file to install the adapter.

**Procedure**

1. Create a temporary directory on the workstation where you want to install the adapter.
2. Extract the contents of the compressed file in the temporary directory.
3. Run the adapter installation wizard. Use the Java™ executable file that comes with Tivoli Directory Integrator to start the installation program. The Java executable file is in the `ITDI_HOME/jvm/jre/bin` directory. Run the following command to start the installation program:

```
ITDI_HOME/jvm/jre/bin/java -jar PosixAdapterInstall_70.jar
```

4. On the Welcome page, click **Next**.

5. In the **Directory Name** field, specify the location of the Tivoli Directory Integrator home directory.

6. Review the installation settings on the Install Summary page and do one of the following steps:
   - Click **Back** to return to a previous page to modify any of the settings.
   - Click **Next** when you are ready to begin the installation.

7. Click **Finish** when the software displays the Install Completed window.

### What to do next

After you finish the adapter installation, do the following actions:

- Verify that the installation completed successfully. See “Installation verification.”
- Import the adapter profile. See “Importing the adapter profile into the IBM Security Identity Manager server” on page 11.
- Create a user account for the adapter on IBM Security Identity Manager. See “Adapter user account creation” on page 13.

### Installation verification

Adapter components are created on the Tivoli Directory Integrator server after you install the adapter.

<table>
<thead>
<tr>
<th>Directory</th>
<th>Adapter component</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ITDI_HOME/jars/</code>connectors</td>
<td>PosixConnector.jar</td>
</tr>
<tr>
<td><code>adapter_solution_directory</code></td>
<td>AIXPConnRes.sh</td>
</tr>
<tr>
<td><code>adapter_solution_directory</code></td>
<td>SolarisPConnRes.sh</td>
</tr>
<tr>
<td><code>adapter_solution_directory</code></td>
<td>HPTrustPConnRes.sh</td>
</tr>
<tr>
<td><code>adapter_solution_directory</code></td>
<td>LinuxPConnRes.sh</td>
</tr>
<tr>
<td><code>adapter_solution_directory</code></td>
<td>LinuxShadowPConnRes.sh</td>
</tr>
<tr>
<td><code>adapter_solution_directory</code></td>
<td>HPNTrustPConnRes.sh</td>
</tr>
<tr>
<td><code>adapter_solution_directory</code></td>
<td>CryptPwd</td>
</tr>
<tr>
<td><code>adapter_solution_directory</code></td>
<td>LastAccessDateReader</td>
</tr>
</tbody>
</table>

Review the installer log files, `POSIXAdapter_Installer.log`, and `POSIXAdapter_Installer_opt.log` that are in the adapter installer directory for any errors.

If this installation is to upgrade a connector, then send a request from IBM Security Identity Manager. Verify that the version number in the `ibmdi.log` matches the version of the connector that you installed. The `ibmdi.log` file is at `ITDI_HOME/adapter_solution_directory/logs`. 
Adapter service start, stop, and restart

To start, stop, or restart the adapter, you must start, stop, or restart the Dispatcher.

The adapter does not exist as an independent service or a process. The adapter is added to the Dispatcher instance, which runs all the adapters that are installed on the same Tivoli Directory Integrator instance.

See the topic about starting stopping, and restarting the dispatcher service in the Dispatcher Installation and Configuration Guide.

Importing the adapter profile into the IBM Security Identity Manager server

Before you can add an adapter as a service, the IBM Security Identity Manager server must have an adapter profile to recognize the adapter.

Before you begin

The files that are packaged with the adapter include the adapter profile JAR file. You can import this adapter profile JAR file as a service profile on the server with the Import feature of IBM Security Identity Manager.

Before you begin to import the adapter profile, verify that the following conditions are met:

• The IBM Security Identity Manager server is installed and running.
• You have root or Administrator authority on IBM Security Identity Manager.

About this task

An adapter profile defines the types of resources that the IBM Security Identity Manager server can manage. Use the profile to create an adapter service on IBM Security Identity Manager server and establish communication with the adapter.

The JAR file includes all the files that are required to define the adapter schema, account form, service form, and profile properties. If necessary, you can extract the files from the JAR file, modify the files, and repackage the JAR file with the updated files.

Procedure

1. Log on to the IBM Security Identity Manager server by using an account that has the authority to do administrative tasks.
2. In the My Work pane, expand Configure System and click Manage Service Types.
3. On the Manage Service Types page, click Import to display the Import Service Types page.
4. Specify the location of the JAR file in the Service Definition File field by doing one of the following actions:
   • Type the complete location of where the file is stored.
   • Use Browse to navigate to the file.
5. Click OK.

Note:
When you import the adapter profile and if you receive an error that is related to the schema, see the trace.log file for information about the error. The trace.log file location is specified by using the handler.file.fileDir property that is defined in the IBM Security Identity Manager enRoleLogging.properties file. The enRoleLogging.properties file is installed in the ITIM_HOME\data directory.

* If you modify any properties in the enRoleLogging.properties file, restart the IBM Security Identity Manager for the change to take effect.

### Adapter profile installation verification

After you install the adapter profile, verify that the installation was successful.

An unsuccessful installation:

* Might cause the adapter to function incorrectly.
* Prevents you from creating a service with the adapter profile.

To verify that the adapter profile is successfully installed, create a service with the adapter profile. For more information about creating a service, see "Creating a service" on page 14.

If you cannot create a service with the adapter profile or open an account on an existing service, the adapter profile is not installed correctly. You must import the adapter profile again.

### Communicating with the Secure Shell protocol

The adapter uses the Secure Shell (SSH) protocol to communicate with the managed resource. This protocol must be installed and running before the adapter connects to the managed resource.

#### About this task

The adapter supports SSH protocol version 2.0. The SSH configuration file lists the SSH protocol version that is supported by your system.

**Note:** OpenSSH is the only supported SSH package on HP-UX and Solaris. OpenSSH and Tectia SSH packages are supported on AIX and Linux systems.

The following list provides information to help you ensure that the UNIX based managed resources in your network can operate with the UNIX and Linux Adapter.

**HP-UX, Linux, and Solaris systems**

SSH is installed and enabled by default on these operating systems. However, check to ensure that the SSH daemon is running before you attempt to connect a managed resource to the IBM Security Identity Manager server. If SSH is not enabled, the connection fails.

**AIX systems**

SSH is not installed on AIX operating systems. If a supported version of SSH is not installed on your system, you might download and install SSH from an open source website. You must install OpenSSL if you are going to use OpenSSH because OpenSSH uses functions that are provided by OpenSSL. Install the OpenSSL first and then install OpenSSH. The AIX operating system requires the OpenSSH product version 4.7 or later.
SSH is installed, check to ensure that the SSH daemon is running. Then, connect the managed resource to the IBM Security Identity Manager server. If SSH is not enabled, the connection fails.

**Note:** On an IPv6 environment, you might be required to configure SSH to listen on an IPv6 address. See the SSH man page on your workstation for detailed information.

**Note:** The following procedure is applicable to OpenSSH packages only.

**Procedure**

1. Open the `sshd_config` file. This file can be found in different locations, depending on the operating system. Common locations are `/etc/ssh` or `/opt/ssh/etc`.
2. Search for the following attributes and use the corresponding settings:

   **Table 6. Secure Shell configuration**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Setting and description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UsePrivilegeSeparation</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Use this setting so that the adapter account is not locked after you do a user account operation.</td>
</tr>
<tr>
<td>ClientAliveInterval</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>This setting disables the <strong>ClientAliveInterval</strong> attribute. The adapter does not acknowledge client-keep-alive messages. If the managed resource sends such messages, the connection is ended as a result.</td>
</tr>
<tr>
<td>PasswordAuthentication</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Use this setting only if you are using password based authentication for your adapter service.</td>
</tr>
</tbody>
</table>

**Adapter user account creation**

You must create a user account for the adapter on the managed resource. You must provide the account information such as administrator name and password when you create the adapter service.

To use SSH to remotely connect to the managed resource, the adapter user account must be one of the following types:

- A root account
- A super user account (SUDO user)
- An account that has root UID permissions

See "Communicating with the Secure Shell protocol" on page 12 for information about SSH.

The adapter user account must have:
Permissions to do user administration tasks, such as add accounts, delete accounts, change passwords for accounts, suspend accounts, restore accounts, and retrieve account data.

Permissions to do group tasks, such as add groups, modify attributes of a group, and delete groups.

For more information about creating a service, see "Creating a service."

Creating a service

After the adapter profile is imported on IBM Security Identity Manager, you must create a service so that IBM Security Identity Manager can communicate with the adapter.

About this task

To create or change a service, you must use the service form to provide information for the service. Service forms might vary depending on the adapter.

Note: If the following fields on the service form are changed for an existing service, the IBM Security Identity Manager adapter service on the Tivoli Directory Integrator server must be restarted.

- User registry
- Use a shadow file?
- Delete home directory when the account is deleted?
- Is sudo user?
- Execute user profile?
- Authentication method
- Passphrase (Required for key-based authentication)
- Private key file (Required for key-based authentication)
- AL File System Path
- Max Connection Count

Procedure

1. Log on to the IBM Security Identity Manager server with an account that has the authority to do administrative tasks.
2. In the My Work pane, click Manage Services and click Create.
3. On the Select the Type of Service page. Select:
   - For AIX operating system: Select POSIX AIX Profile.
   - For HP-UX operating system: Select POSIX HP-UX Profile.
   - For Solaris operating system: Select POSIX Solaris Profile.
   - For Linux operating system: Select POSIX Linux Profile.
4. Click Next to display the adapter service form.
5. Complete the following fields on the service form.
   - On the General Information tab:
Service Name
Specify a name that defines the adapter service on the IBM Security Identity Manager server.

Note: Do not use forward (/) or backward slashes (\) in the service name.

Description
Optionally, specify a description that identifies the service for your environment.

IBM Tivoli Directory Integrator URL
Optionally, specify the URL for the Tivoli Directory Integrator instance. The valid syntax for the URL is rmi://ip-address:port/ITDIDispatcher, where ip-address is the Tivoli Directory Integrator host and port is the port number for the Dispatcher.

The default for version 7.1 is this URL:
rmi://localhost:1099/ITDIDispatcher

For information about changing the port number, see IBM Security Dispatcher Installation and Configuration Guide.

Managed resource location
Specify the IP address or host name of the managed resource. This location uses the default SSH port, which is port 22. If the SSH port is different, then ip/host:port can be used.

Note: An IPv6 address must be enclosed in brackets. An example of a valid IPv6 address format is [fedc:ba98:7654:3210:fedc:ba98:7654:3210]:22

RXA Internal Command TimeOut
Specify a value, in milliseconds, to control how long the adapter waits for a response after a remote command is issued to a managed resource. The default value is 5000 milliseconds. Modify this default value if operations on the managed resource timeout frequently.

User registry
This input field is available only on service forms for AIX profiles. This adapter supports user management and authentication by using files or by using LDAP.

Note:
• This field is case-sensitive.
• AIX roles are not reconciled or managed by the adapter for any AIX service with a user registry that is defined as LDAP.
  a. If the users on the managed resource are to be managed only through the /etc/password file, leave the field blank.
  b. If this setup is a mixed and the users are to be managed through the /etc/password file, type files.

Note: A mixed setup means that some users on the managed resource are defined in LDAP and some users are defined in files. These users are mutually exclusive and cannot be managed by a single service. If you want IBM
Security Identity Manager to manage users that are defined in LDAP as well, ensure that you also create a service to manage users through LDAP.

c. If this setup is a mixed setup and the users are to be managed through LDAP, type LDAP.

Note: A mixed setup means that some users on the managed resource are defined files and some users are defined in LDAP. These users are mutually exclusive and cannot be managed by a single service. If you want IBM Security Identity Manager to manage users that are defined in files as well, ensure that you also create a service to manage users through files.

Use a shadow file?
Select this check box if shadow passwords are enabled on the managed resource. This field applies to service forms only when you use the Linux or HP-UX service profiles.

For Linux operating systems, shadow passwords are enabled by default. When you create a service for HP-UX, by default the Use a shadow file? field is enabled. If the HP-UX system you are connecting to is an HP-UX trusted system, then the Use a shadow file? field is irrelevant and the adapter ignores the field.

Delete home directory when the account is deleted?
Select this check box if you want the home directory of the user to be deleted when the user is deleted.

Owner
Optionally specify a IBM Security Identity Manager user as a service owner.

Service Prerequisite
Optionally, specify a IBM Security Identity Manager service that is a prerequisite to this service.

On the Additional Configuration tab:
This tab applies only to Linux systems.

Command used to query failed logins
Specifies the system command that is used to detect and tally failed login attempts and enforce account lockout. This command must be configured through the PAM mechanism. If no value is specified, the default faillog command is used. This command is not available on some operating systems, such as RHEL 6.1 and later versions.

File or directory where failed login records are found
Specifies the absolute path to the location of the failed login attempt datastore, if it is not the default datastore. This field applies to faillock and pam_tally2 only. The field is ignored when faillog is used.

Maximum failed logins allowed
Specifies the maximum number of failed logins that can occur before an account is locked. This field applies to faillock and pam_tally2 only. The field is ignored when faillog is used.
Administrator name

Specify the user name for the administrator. If you are specifying a super user, instead of a root user, see Appendix C, “Super user creation on a supported operating system,” on page 73.

Is sudo user?

Select this check box if the administrator name is a super user. Sudo user privileges must be carefully configured on the resource. For more information about sudo users, see Appendix C, “Super user creation on a supported operating system,” on page 73.

Execute user profile?

Available for HP-UX services only.

Click this check box to run the profile of the adapter user before you run operations on the endpoint.

When you create a service for HP-UX, by default the Execute user profile? field is disabled. You might want to enable this field if the adapter user profile remaps special terminal control characters on HP-UX (for example @ and #). The profile can remap these characters when the Execute user profile? field is enabled. In this case, you can use those special characters in passwords when you add or change accounts. If the field is not enabled and you use a special character, the add or modify operations for the account fail when the password is set.

Running the user profile can affect the runtime environment of the adapter at the endpoint and the outcome of adapter operations. Running the profile has some limitations and must be used with care. For example:

- Do not call another shell from the profile scripts. Doing so can cause the remote operation to hang.
- Do not echo any strings from the profile when you trap signals. The profile must not echo any output from trap commands. The echoed string might be merged with the results of the command that is running.

Use the default settings for the owner, group, and permissions settings on both the /etc/profile and the adapter user .profile file. Changing the values for these attributes can cause the remote operation to fail.

Authentication method

From the drop-down menu, select the authentication method to be used by the adapter when it communicates with the managed resource for user management. Select Password-Based Authentication or Key-Based Authentication. For more information about key-based authentication, see Appendix D, “Key-based authentication for the UNIX and Linux Adapter,” on page 85.

Note: This authentication method is only for adapter communication and does not apply to users created on the managed resource by this adapter.
Password
Required for password-based authentication: Specify the password for the administrator.

Passphrase (Required for key-based authentication)
Specify the pass-phrase that is associated with the private key. For more information about private keys, see “Enabling RSA key-based authentication on UNIX and Linux operating systems” on page 85.

Private key file (Required for key-based authentication)
Specify the full path and file name of the keystore that contains the private key of the client. This keystore must be on the workstation that runs the Tivoli Directory Integrator server. For more information about keystore, see Appendix D, “Key-based authentication for the UNIX and Linux Adapter,” on page 85.

On the Dispatcher Attributes tab:

AL FileSystem Path
Specify the file path from where the dispatcher loads the assembly lines. If you do not specify a file path, the dispatcher loads the assembly lines that are received from IBM Security Identity Manager. You can specify the following file path to load the assembly lines from the profiles directory of the Windows operating system: c:\Files\IBM\TDI\TDI_VERSION\profiles or you can specify the following file path to load the assembly lines from the profiles directory of the UNIX and Linux operating systems: system:/opt/IBM/TDI/TDI_VERSION/profiles

Max Connection Count
Specify the maximum number of assembly lines that the dispatcher can run simultaneously for the service. If you enter 0 in the Max Connection Count field, the dispatcher does not limit the number of assembly lines that run simultaneously for the service.

Disable AL Caching
Select the check box to disable the assembly line caching for add, modify, and delete operations in the dispatcher for the service.

On the Status and information tab
Contains read only information about the adapter and managed resource. These fields are examples. The actual fields vary depending on the type of adapter and how the service form is configured. The adapter must be running to obtain the information. Click Test Connection to populate the fields.

Last status update: Date
Specifies the most recent date when the Status and information tab was updated.

Last status update: Time
Specifies the most recent time of the date when the Status and information tab was updated.

Managed resource status
Specifies the status of the managed resource that the adapter is connected to.
Adapter version
Specifies the version of the adapter that the IBM Security Identity Manager service uses to provision request to the managed resource.

Profile version
Specifies the version of the profile that is installed in the IBM Security Identity Manager server.

TDI version
Specifies the version of the Tivoli Directory Integrator on which the adapter is deployed.

Dispatcher version
Specifies the version of the Dispatcher.

Installation platform
Specifies summary information about the operating system where the adapter is installed.

Adapter account
Specifies the account that running the adapter binary file.

Adapter up time: Date
Specifies the date when the adapter started.

Adapter up time: Time
Specifies the time of the date when the adapter started.

Adapter memory usage
Specifies the memory usage for running the adapter.

If the connection fails, follow the instructions in the error message. Also

- Verify the adapter log to ensure that the IBM Security Identity Manager test request was successfully sent to the adapter.
- Verify the adapter configuration information.
- Verify IBM Security Identity Manager service parameters for the adapter profile. You can verify the work station name or the IP address of the managed resource and the port.

6. Click Finish.
Chapter 4. Adapter installation and uninstallation in silent mode

You can use the \texttt{-i silent} option to install or uninstall the adapter in silent mode.

Silent installation suppresses the adapter installation wizard and the Launcher User Interfaces (UIs). It does not display any information or require interaction.

Installing the adapter in silent mode

You can either use the default settings or override those settings when you install the adapter in silent mode.

\textbf{About this task}

If you accept the default setting for the silent installation, the adapter is installed in a location that depends on your operating system.

\textbf{Windows operating systems}

\%SYSTEM\_DRIVE\_ROOT\%\Program Files\IBM\TDI\V7.1

\textbf{UNIX and Linux operating systems}

/opt/IBM/TDI/V7.1

You can override the default settings with the \texttt{-D} parameter. The \texttt{-D} must be followed immediately by an option-value pair. No space exists after \texttt{-D}.

\textbf{Note}: If an argument contains spaces, you must wrap the argument in quotation marks.

\begin{table}[h]
\centering
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\texttt{-DUSER_INSTALL_DIR}</td>
<td>This parameter overrides the default installation path. For example, \texttt{-DUSER_INSTALL_DIR=&quot;D:\security/MyFolder&quot;}</td>
</tr>
<tr>
<td>\texttt{-DFORCE_DISPATCHER_SERVICE_START_ONINSTALL}</td>
<td>If the dispatcher service is running before the installation, the installer stops the service. It restarts the service after the installation is completed. If the dispatcher service is not running before the installation, use this parameter to start the service after the installation. Set the value of the parameter to \texttt{YES}.</td>
</tr>
</tbody>
</table>
\end{table}

\textbf{Procedure}

1. Go to a command line.
2. Run either of the following commands:
   \begin{itemize}
   \item To install the adapter in silent mode with the default settings, issue the command:
     \texttt{java -jar PosixAdapterInstall_70.jar -i silent}\
   \item To install the adapter in silent mode with customized settings, use the following command:
     \texttt{java -jar PosixAdapterInstall_70.jar -i silent -DUSER\_INSTALL\_DIR="D:\security/MyFolder" -DFORCE\_DISPATCHER\_SERVICE\_START\_ONINSTALL=YES}\
   \end{itemize}
To install the adapter in silent mode and changing one or more default settings, use the `-D` parameter. For example, this command overrides the default installation directory for a Windows operating system.

```java
java -jar PosixAdapterInstall_70.jar -i silent
-DUSER_INSTALL_DIR="E:\Program Files\IBM\TDI\V7.1"
```

**Results**

The adapter is installed in the adapter installation directory.

---

## Uninstalling the adapter in silent mode

You can uninstall the adapter without any prompts for user action.

**About this task**

Run the command from the `PosixAdapterUninstall` directory in the installation directory of the adapter. If you run the command from a different directory, you must specify the full file path to the `uninstaller.jar` file. For example, this command is run from outside the `PosixAdapterUninstall` directory.

```java
java
-jar "E:\Program Files\IBM\TDI\V7.1\PosixAdapterUninstall\uninstaller.jar"
-i silent
```

**Table 8. silent mode parameter for uninstalling**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-DFORCE_DISPATCHER_SERVICE_START_ONUNINSTALL</code></td>
<td>If the dispatcher service is running before the uninstallation, the installer stops the service. It restarts the service after the uninstallation is completed. If the dispatcher service is not running before the uninstallation, use this parameter to start the service after the uninstallation. Set the value of the parameter to <code>YES</code>.</td>
</tr>
</tbody>
</table>

**Procedure**

1. Go to a command line.
2. Run either of the following commands:
   
   - To uninstall the adapter with the default settings, run the command:
     ```java
     java -jar uninstaller.jar -i silent
     ```
   - To ensure that the dispatcher service is restarted after you uninstall the adapter, run the command:
     ```java
     java -jar uninstaller.jar -i silent
     -DFORCE_DISPATCHER_SERVICE_START_ONUNINSTALL=yes
     ```

**Results**

The adapter is removed without any additional user response or interaction.
Chapter 5. First steps after installation

After you install the adapter, you must do several other tasks. The tasks include configuring the adapter, setting up SSL, installing the language pack, and verifying that the adapter works correctly.

Adapter configuration

You can use the configuration options for the UNIX and Linux Adapter.

- “Customizing the adapter profile”
- “Running user-defined scripts” on page 25
- “Customizing the adapter profile”
- “Running user-defined scripts” on page 25
- “Customizing password prompt attributes” on page 29
- “User home directory creation” on page 28
- “Adding home directory permissions on the account form” on page 30
- “Editing adapter profiles on the UNIX or Linux operating system” on page 28
- “Adapter features customization and extension” on page 28
- “Setting up locales” on page 32

See the IBM Security Dispatcher Installation and Configuration Guide for more configuration options such as:

- JVM properties
- Dispatcher filtering
- Dispatcher properties
- Dispatcher port number
- Logging configurations
- Secure Sockets Layer (SSL) communication

Customizing the adapter profile

To customize the adapter profile, you must change the adapter profile JAR file. You might customize the adapter profile to change the account form or the service form. You can also change the labels on the forms by using the Form Designer or the CustomLabels.properties file. Each adapter has a CustomLabels.properties file.

About this task

The adapter profile JAR file is included in the adapter compressed file that you downloaded from the IBM website. The JAR file and the files that are contained in the JAR file vary depending on your operating system.

Note: You cannot modify the schemas for this adapter. Attributes cannot be added to or deleted from the schema.

AIX (PosixAixProfile.jar)

The following files are included in the AIX profile JAR file:

- CustomLabels.properties
- erPosixAixAccount.xml
HP-UX (PosixHpuxProfile.jar)
The following files are included in the HP-UX profile JAR file:
- CustomLabels.properties
- erPosixHpuxAccount.xml
- erPosixHpuxRMIService.xml
- posixAdd.xml
- posixDelete.xml
- posixModify.xml
- posixSearch.xml
- posixTest.xml
- schema.dsml
- service.def
- posixGroupAdd.xml
- posixGroupDelete.xml
- posixGroupModify.xml
- posixRoleAdd.xml
- posixRoleDelete.xml
- posixRoleModify.xml

Solaris (PosixSolarisProfile.jar)
The following files are included in the Solaris profile JAR file:
- CustomLabels.properties
- erPosixSolarisAccount.xml
- erPosixSolarisRMIService.xml
- posixAdd.xml
- posixDelete.xml
- posixModify.xml
- posixSearch.xml
- posixTest.xml
- schema.dsml
- service.def
- posixGroupAdd.xml
- posixGroupDelete.xml
- posixGroupModify.xml
Linux (PosixLinuxProfile.jar)

The following files are included in the Linux profile JAR file:
- CustomLabels.properties
- erPosixLinuxAccount.xml
- erPosixLinuxRMIService.xml
- posixAdd.xml
- posixDelete.xml
- posixModify.xml
- posixSearch.xml
- posixTest.xml
- schema.dsml
- service.def
- posixGroupAdd.xml
- posixGroupDelete.xml
- posixGroupModify.xml

After you edit the file, you must import the file into the IBM Security Identity Manager server for the changes to take effect.

Procedure

1. Edit the profile JAR file.
   a. Log in to the system where the UNIX and Linux Adapter is installed.
   b. Copy the JAR file into a temporary directory.
   c. Extract the contents of the JAR file into the temporary directory. Run the following command. The following example applies to the Linux adapter profile. Type the name of the JAR file for your operating system.

```
# cd /tmp
# jar -xvf PosixLinuxProfile.jar
```

   The `jar` command extracts the files into the PosixLinuxProfile directory.
   d. Edit the file that you want to change.
   e. Save the file.

2. Import the file.
   a. Create a JAR file by using the files in the /tmp directory. Run the following command:

```
# cd /tmp
# jar -cvf PosixLinuxProfile.jar PosixLinuxProfile
```

   b. Import the modified profile JAR file into the IBM Security Identity Manager application server. For more information about importing the JAR file, see “Importing the adapter profile into the IBM Security Identity Manager server” on page 11.

   c. Stop and start the IBM Security Identity Manager server.
   d. Stop and start the UNIX and Linux Adapter service. See “Adapter service start, stop, and restart” on page 11 for information about stopping and starting the UNIX and Linux Adapter service.

Running user-defined scripts

The UNIX and Linux Adapter is configured to run user-defined scripts before a request is processed (preexec), after a request is processed (postexec), or both.
About this task

Running user-defined scripts can be useful when external activities are required to manage the resource. Use these attributes that are defined in the relevant Posix account form:

- Pre-execution options:
  - `erPosixPreExec`
    Always continue the operation regardless of the pre-execution script outcome (succeed or fail).
  - `erPosixPreExecRunOption`
    Continue the operation only when the pre-execution script succeeds.

- Post-execution options:
  - `erPosixPostExec`
    Always continue the operation regardless of the post-execution script outcome (succeed or fail).
  - `erPosixPostExecRunOption`
    Continue the operation only when the post-execution script succeeds.

Note:
1. The term operation refers to any account management request. For example, `user add` or `user modify`.
2. The status or outcome of the `preexec` and `postexec` commands are not returned to the IBM Security Identity Manager server.
3. On a modify request, the IBM Security Identity Manager server sends only those attributes whose values are changed. This behavior differs from an add operation in which all the attributes are always sent. The modify behavior applies to the `preexec` and `postexec` attributes.

To send these attributes on a modify operation regardless of actual value changes, update the `service.def` file for the relevant Posix adapter profile.

Procedure
1. Extract the adapter profile JAR file. For example, `PosixAIXProfile.jar`
2. Open the `service.def` file in a text editor.
3. Insert the following lines in `service.def`, under `<operation cn="posixModify">`

   ```xml
   <input name="erPosixPreExec" source="erPosixPreExec"></input>
   <input name="erPosixPostExec" source="erPosixPostExec"></input>
   <input name="erPosixPreExecRunOption" source="erPosixPreExecRunOption"></input>
   <input name="erPosixPostExecRunOption" source="erPosixPostExecRunOption"></input>
   ```

4. Save the changes and create another adapter profile JAR file.
   ```bash
   jar -cvf PosixAixProfile.jar PosixAixProfile
   ```

Defining the maximum connection count for adapter operations

You can limit the number of connections that can be made to a resource based on the service, service type, and operation. You can modify the `service.def` file in the service profile. Alternatively, you can specify a value for the Max Connection Count field on the service form of a resource.
About this task

Limit the number of concurrent connections to a resource if you see errors that are caused by contention for files or other objects on the resource. For example, when many operations occur at the same time for account add, some might fail because they cannot get write access to the /etc/passwd file. To reduce contention, lower the maximum connection count for the resource or the add operation.

To set a default or an absolute maximum connection count for a service type, modify the service.def file. A default count can be overridden on a per-resource basis; an absolute count cannot be overridden.

To change the service.def file, take these steps:

Procedure
1. Extract the adapter profile JAR file. For example, extract PosixAIXProfile.jar with this command:
   
   `jar -xvf PosixAixProfile.jar`

2. Open the service.def file in a text editor.

3. To limit the maximum connections for an operation type, first locate the type. A maximum connection count is defined for each operation type such as add (posixAdd) or modify (posixModify). Locate the type of operation whose maximum connection count you want to set. For example, locate the posixModify operation:

   `<operation cn="posixModify">`

4. Find the `<dispatcherParameter name="MaxConnectionCnt"...>` element under the posixModify operation entry.

5. Edit the dispatcherParameter element to specify a default value or an absolute value.

   • Specify a default value.
   
   Create an entry similar to this example:

   `<dispatcherParameter name="MaxConnectionCnt" source= "erPosixMaxConnectionCnt">
   <default>value</default>
   </dispatcherParameter>`

   For any AIX resource, the maximum number of concurrent operations for account modify has a default of value. To override this default, specify a different value in the Max Connection Count field on the Dispatcher Attributes tab of the service form of the AIX resource.

   • Specify an absolute value.

   Create an entry similar to this example:

   `<dispatcherParameter name="MaxConnectionCnt">
   <value>value</value>
   </dispatcherParameter>`

   For any AIX resource, the maximum number of concurrent operations for account modify is value, which cannot be overridden.

Note:

• The maximum number of connections for search (recon) operations is always one, regardless of the settings in the service.def file or on the service form.

• If no maximum connection count is defined in the service.def file or on the service form, the connection count is unlimited.

6. Save the changes and create another adapter profile JAR file. For example:

   `jar -cvf PosixAixProfile.jar PosixAixProfile`
7. Import the modified profile JAR file into IBM Security Identity Manager.

User home directory creation

The UNIX and Linux Adapter provides a user-selectable option to create a default home directory for a user or an account.

The default home directory is created by concatenating the base directory value that is defined on that system with the account name or user name to be created.

Example

The base directory value on the target system is /home. The user name for the account that is being created is testuser. The default home directory is /home/testuser.

Note: AIX systems ignore this option. The AIX operating systems create a home directory by default for each new account.

Editing adapter profiles on the UNIX or Linux operating system

The adapter profile .jar file might contain ASCII files that are created by using the MS-DOS ASCII format.

About this task

If you edit an MS-DOS ASCII file on the UNIX operating system, you might see a character ^M at the end of each line. These characters indicate new lines of text in MS-DOS. The characters can interfere with the running of the file on UNIX or Linux systems. You can use tools, such as dos2unix, to remove the ^M characters. You can also use text editors, such as the vi editor, to remove the characters manually.

Example

You can use the vi editor to remove the ^M characters. From the vi command mode, run the following command and press Enter:

:\%s/^M//g

When you use this command, enter ^M or Ctrl-M by pressing ^v^M or Ctrl V Ctrl M sequentially. The ^v instructs the vi editor to use the next keystroke instead of issuing it as command.

Adapter features customization and extension

The IBM Security Identity Manager adapters can be customized or extended or both. The type and method of this customization varies depending on the adapter.

Customizing and extending adapters requires a number of skills. The developer must be familiar with the following concepts and skills:

- IBM Security Identity Manager administration
- IBM Tivoli Directory Integrator management
- Tivoli Directory Integrator Assembly Line development
- LDAP schema management
- Working knowledge of Java scripting language
• Working knowledge of LDAP object classes and attributes
• Working knowledge of XML document structure

**Note:** If the customization requires a new Tivoli Directory Integrator connector, the developer must also be familiar with Tivoli Directory Integrator connector development and working knowledge of Java programming language.

**IBM Security Identity Manager resources**
See the “Learn” section of the [IBM Security Identity Manager Support website](https://www.ibm.com/support/pages/ibm-securitiy-identity-manager) for links to training, publications, and demonstrations.

**Tivoli Directory Integrator resources**
See the “Learn” section of the [Tivoli Directory Integrator Support website](https://www.ibm.com/support/pages/tivoli-directory-integrator) for links to training, publications, and demonstrations.

**IBM Security Identity Manager adapter development resources**

**Adapter Development Tool**
The Adapter Development Tool (ADT) is a tool that is used by IBM Security Identity Manager customers and consultants to create custom IBM Security Identity Manager adapters. It reduces adapter delivery time and it helps in the development of custom adapters. The ADT is available from the [IBM Open Process Automation Library (OPAL) website](https://www.ibm.com/software/developer/opal).

**Support for customized adapters**

The integration to the IBM Security Identity Manager server, the adapter framework, is supported. However, IBM does not support the customizations, scripts, or other modifications. You might experience a problem with a customized adapter. In this case, IBM Support might require the problem to be demonstrated on the GA version of the adapter before a PMR is opened.

### Optional feature configuration

Depending on your needs, the adapter has attributes that you can optionally configure for the following capabilities.

**Customizing password prompt attributes**
The UNIX and Linux Adapter does password changes by using an interactive Secure Shell (SSH) session. The adapter searches for the default password prompts on the managed resource to complete the transaction successfully. If the managed resource has customized password prompts, then you can specify the password prompts on the service form that the adapter must search for.

**About this task**
The password prompt attributes are:

- `erPosixNewRegx` - the new password prompt
- `erPosixRetypeRegx` - the retype password prompt

To customize these password prompt attributes on the service form, do the following steps from IBM Security Identity Manager. The customized password prompt attributes are displayed on the service form. The adapter does a case-insensitive match on these password prompts.
**Procedure**

1. Log on to IBM Security Identity Manager as an administrator.
2. In the My Work pane, expand **Configure System** and click **Design Forms** to display the Design Forms page.
3. From the applet, double-click **Service** to display the service form profiles.
4. Double-click the service form profile whose service form you want to customize. Select one of the following profiles:

   **POSIX AIX account**
   Select this option to customize the `erPosixNewRegx` and `erPosixRetypeRegx` attributes on the AIX service form. The default values of these attributes on this account are:
   ```
   erPosixNewRegx = ".*new password:\$"
   erPosixRetypeRegx = "re-enter .* new password:\$"
   ```

   **POSIX HP-UX account**
   Select this option to customize the `erPosixNewRegx` and `erPosixRetypeRegx` attributes on the HP-UX service form. The default values of these attributes on this account are:
   ```
   erPosixNewRegx = ".*new password:\$"
   erPosixRetypeRegx = ".*re-enter new password:\$"
   ```

   **POSIX Linux account**
   Select this option to customize the `erPosixNewRegx` and `erPosixRetypeRegx` attributes on the Linux service form. The default values of these attributes on this account are:
   ```
   erPosixNewRegx = ".*new password:\$"
   erPosixRetypeRegx = ".*re-enter new password:\$"
   ```

   **POSIX Solaris account**
   Select this option to customize the `erPosixNewRegx` and `erPosixRetypeRegx` attributes on the Solaris service form. The default values of these attributes on this account are:
   ```
   erPosixNewRegx = ".*new password:\$"
   erPosixRetypeRegx = ".*re-enter new password:\$"
   ```

5. From the Attributes List window, double-click the `erPosixNewRegx` attribute to add it to the service form.
6. From the Attributes List window, double-click the `erPosixRetypeRegx` attribute to add it to the service form.
7. Click **Save Form Template** icon. After you customize the password prompt attributes, the following attributes are available on the service form:
   - New Password Regular expression
   - Retype Password Regular expression

**Adding home directory permissions on the account form**

You might want to add or modify the home directory permissions of the user on the managed resource.

**About this task**

To modify the home directory permissions, you must customize the `erPosixHomeDir` attribute on the account form. Do the following steps on IBM Security Identity Manager:
Procedure
1. Log on to IBM Security Identity Manager as an administrator.
2. In the My Work pane, expand Configure System and click Design Forms to display the Design Forms page.
3. From the applet, double-click Account to display the account form profiles.
4. Double-click the account form profile to add the erPosixHomeDir attribute on the account form. Select one of the following profiles:
   - POSIX AIX account
     Select this option to customize the erPosixHomeDir attribute on the AIX account form.
   - POSIX HP-UX account
     Select this option to customize the erPosixHomeDir attribute on the HP-UX account form.
   - POSIX Linux account
     Select this option to customize the erPosixHomeDir attribute on the Linux account form.
   - POSIX Solaris account
     Select this option to customize the erPosixHomeDir attribute on the Solaris account form.
5. From the Attributes List window, double-click the erPosixHomeDir attribute to add it to the $tabemployeeinfo tab.
6. Right-click erposixperhomedir and click Change To>UMask.
7. Click the Save Form Template icon. After you customize the attribute, the Home directory permissions attribute is available on the account form.

Adding umask settings on the account form
You might want to add or modify the umask permissions of the user on the managed resource. The umask settings control how file permissions are set for newly created files.

About this task
To modify the umask permissions, you must customize the erPosixUmask attribute on the account form. Do the following steps on IBM Security Identity Manager:

Procedure
1. Log on to IBM Security Identity Manager as an administrator.
2. In the My Work pane, expand Configure System and click Design Forms to display the Design Forms page.
3. From the applet, double-click Account to display the account form profiles.
4. Double-click the account form profile to add the erPosixUmask attribute on the account form. Select one of the following profiles:
   - POSIX AIX account
     Select this option to customize the erPosixUmask attribute on the AIX account form.
   - POSIX HP-UX account
     Select this option to customize the erPosixUmask attribute on the HP-UX account form.
**POSIX Linux account**
Select this option to customize the `erPosixUmask` attribute on the Linux account form.

**POSIX Solaris account**
Select this option to customize the `erPosixUmask` attribute on the Solaris account form.

5. From the Attributes List window, double-click the `erPosixUmask` attribute to add it to the $tabemployeeinfo tab.

6. Right-click `erPosixUmask` and click Change To>UMask.
7. Click the Save Form Template icon. After you customize the attribute, you can use it when you create or modify a user account.

Locate the attribute that is labeled `UNIX umask` on the account form and use the Access Type permission boxes to change or set the read, write and execute permissions for user, group and other access.

### Setting up locales

You can specify a particular code page for the adapter to use when encoding and decoding data. By default, the adapter uses the same locale and code page that are specified for the administrative user account that the adapter uses on the managed resource. The locale and code page are typically the same as the system locale and code page. If the locales and code pages are different, use this task to configure the adapter to use the system locale and code page.

### About this task

The `erPosixEncoding` attribute provides enhanced support in the Posix adapter for characters sets from user-specified locales.

### Procedure

1. Open the DESIGN FORMS feature of the IBM Security Identity Manager server. Click Configure System > Design Forms.
2. Click Service and select a POSIX Profile.
3. Add the attribute `erposixencoding` on the Service form from the Attribute List.
4. Save the form and close the Design Form window.
5. Create a service with following parameter:

   ```
   Code Page to be used for data encoding(Default to UTF-8) : Code page for data
   ```

   *Code page for data* on the service form is the corresponding code page to the LOCALE in use. For example, the code page for the German locale is ISO-8859-1.

   ```
   Code Page to be used for data encoding(Default to UTF-8) : ISO-8859-1
   ```

### Configuring alternative adapter scripts location

You can specify where the adapter script files are stored on the managed UNIX or Linux system.

### Before you begin

The administrator that is defined on the service form for the managed system must have sufficient permission to access the specified location or directory.
About this task

A configurable option, erPosixCopyAdpFilesTo, can be used to store adapter script files in a location other than the default location /tmp. This option is configurable by service and is not automatically displayed on the service form.

To add this attribute:

**Procedure**

1. Open the DESIGN FORMS feature of the IBM Security Identity Manager server. Click **Configure System > Design Forms**.
2. Click **Service** and select any POSIX Profile.
3. Add the attribute erPosixCopyAdpFilesTo on the **Service** form from the **Attribute List**.
4. Save the form.
5. Create a service with following parameter:

   ```
   Location of temporary files on resource : full path to file location
   ```

**Reconciling with custom scripts**

You can run reconciliation with either the reconciliation script bundled with the adapter or your own customized reconciliation script that is optimized for your setup.

**Before you begin**

Ensure that these conditions are true:

- The customized reconciliation script name is user definable, and must be present in the `timsol` folder.
- You must have executable permission on reconciliation script. You must have similar permissions on the specified folder as on the `/tmp` folder.
- The reconciliation script and folder cannot contain double quotation marks or spaces.
- The names of the reconciliation script and folder must follow the naming conventions of the operating system.

**About this task**

To use this feature, select the **Use recon script from this folder on managed resource** attribute on the service form. The adapter uses the reconciliation script present at that location. If this option is not selected, then the standard reconciliation script that is bundled with the adapter is used.

**Note:**

1. If a value for both **Location of temporary files on resource** and **Use recon script from this folder on managed resource** are selected, then **Use recon script from this folder on managed resource** is used.
2. If a folder is specified on the managed resource without a script file name, the adapter looks for the standard reconciliation script name. The script name is based on the operating system type in the specified folder. On an AIX operating system, if the file path given for this attribute is `/reconfolder`, the adapter looks for the `/reconfolder/AixPConnRes.sh` file.
**Procedure**

1. Open the DESIGN FORMS feature of the IBM Security Identity Manager server. Click **Configure System** > **Design Forms**.
2. Click **Service** and select **POSIX Solaris Profile**.
3. Add the attribute **erPosixReconScriptLocation** on the Service form from the Attribute List.
4. Save the form.

**Ending a user session after suspension**

The adapter can be configured to end active user sessions after the user is suspended.

**About this task**

The default behavior of the adapter is not to end active sessions after the user is suspended. Use this task to configure the adapter to end active sessions after the successful completion of a suspension request.

This option is configurable by service. The option is not displayed automatically on the Service Form.

**Note:**

1. This option must not be used on systems that allow duplicate user IDs.
2. An error condition or hang occurs if a user attempts to suspend itself when this option is set.

To add this attribute to the Service Form:

**Procedure**

1. Open the DESIGN FORMS feature of the IBM Security Identity Manager server. Click **Configure System** > **Design Forms**.
2. Click **Service** and select any **POSIX Solaris Profile**.
3. Add the attribute **erPosixKillUserProcess** on the Service form from the Attribute List.
4. Change display type to **CheckBox** and save the form.
5. Create a service with following parameter:
   - **Kill active user process on suspending an account**
6. Restart the Dispatcher.

**Ending user processes to delete a user account**

On a Linux operating system, you cannot delete a user if any user processes are running. The adapter can be configured for Linux operating systems to end all user processes when a user is deleted.

**About this task**

The default behavior of the Linux operating system is to fail a user delete request if any user processes are running. Use this task to configure the adapter to end any active user processes when you submit a delete user request.

This option is configurable by service. The option is not displayed automatically on the Service Form.
Note: This option must not be used on systems that permit duplicate user IDs.

To add this attribute to the Service Form:

**Procedure**

1. Open the DESIGN FORMS feature of the IBM Security Identity Manager server. Click **Configure System > Design Forms**.
2. Click **Service** and select any **POSIX Linux Profile**.
3. Add the attribute **erPosixDelUserInUse** on the Service form from the **Attribute List**.
4. Change display type to **CheckBox** and save the form.
5. Create a service with following parameter:
   - Delete user account even when it is in use
6. Restart the Dispatcher.

**Configuring last access date support for Solaris systems**

You can configure the UNIX and Linux Adapter to show the date that an account on a Solaris system was last accessed.

**About this task**

You can add two fields to the service form:

**Retrieve last Access Date?**

The value for **erPosixLastAccessDateBinaryCopy** is either TRUE or FALSE. The value of this option determines how the adapter handles "Account last accessed on" attribute. This value must be set to TRUE on the service form for the adapter to retrieve the value for "Account last accessed on". The adapter copies the LastAccessDateReader binary file to a specified location or to the /tmp folder (default location) during reconciliation. After reconciliation, the adapter deletes the binary file from the resource. This binary file is used to read the contents of the /var/adm/wtmpx file to retrieve the last access date for the user accounts.

**Account last accessed on**

The value for the **erPosixLastAccessDate** is retrieved from the /var/adm/wtmpx file that is maintained on the Solaris system. This file contains history of user access and administrative information. The minimum permissions that are required to read this file is 0644 (rw-r--r--).

**Note:** The **erPosixLastAccessDate** attribute that is added to account from by using the Design Forms editor must be kept as **Read-Only on Modify**.

The **Account last accessed on** field has these behaviors for the following operations:

- **Add**
  - When a user account is requested with the "Account last accessed on" value on the Account Form, the adapter does not set this value. The adapter returns a message: Not supported during add operation.

- **Modify**
  - The value is read only.
Reconciliation
The adapter reconciles the value for each account in GMT format (for example 20110102122500Z).

To add these attributes to the Service Form:

Procedure
2. Click Service and select POSIX Solaris Profile.
3. Add the attribute erposixlastaccesdatebinarycopy on the service form from the Attribute List.
4. Change display type to CheckBox and save the form.
5. Click Account and select POSIX Solaris Account.
6. On the account form, add the attribute erposixlastaccesdate from the Attribute List.
7. Click the Read-Only on Modify check box in the format tab under the properties section.
8. Save the form and close the Design Form window.

Non-login account (passwd-N) support
The adapter supports "No Password" accounts. A "No Password" account does not have a password. Accounts without passwords cannot be used to log in to the system interactively with commands such as login, telnet, ftp, or ssh.

The adapter supports "No Password" accounts on Solaris 10 and higher and HP-UX Trusted and Non-Trusted operating systems.

The Is No Password Account? check box on the account form is used to enable and disable the behavior. The possible values for this option are TRUE when selected and FALSE when not selected. When the option is selected, adapter creates a "No Password" account. The adapter creates a "Password" account when the option is not selected.

Note:
1. Password aging attributes for "No Password" accounts on HP-UX Trusted operating systems cannot be set.
2. When run from a sudo-super user account, HP-UX systems require these conditions.
   • /usr/sam/lbin and /usr/bin be in the user path.
   • /usr/sam/lbin/usermod.sam and /usr/bin/test be in the user entry in the sudoers file.

Attribute usage
The following examples demonstrate the usage of the attribute in various operations:

Add A new user account can be requested with the Is No Password Account? option that is selected on the account form. In this case, the adapter creates a "No Password" account on Solaris 10 and higher and HP-UX Trusted and Non-Trusted operating systems.
Modify
When an account is modified with the option selected on the account form, the account is set to "No Password". When the option is not selected, the adapter sets the account to "Password". In this case, a password must also be provided.

Note: Changing an account from No Password to Password is not available through the UI. An error is returned: Cannot change No Password Accounts to Password Accounts without password.

This modify operation can be done only through Workflows by providing a password along with a value of FALSE for erPosixNpAccount.

Password change
A change password request is valid for "Password" accounts only.

Suspend
The suspend operation for “No Password” accounts works similar to “Password” accounts.

Restore
Restore operation for “No Password” accounts is as follows:
- "No Password” accounts on Solaris 10 and HP-UX Trusted operating systems can be restored. However, a password cannot be set. If a password is supplied in the restore request, the Can't set password for No Password Accounts error is returned.
- After a “No Password” account is restored on HP-UX Non-Truste systems, the resource requires a new password at the next user login. Because of HP-UX Non-Truste resource behavior, the adapter is not able to distinguish a “Password” account from a “No Password” account on subsequent reconciliation requests. Therefore, use caution when you suspend and restore “No Password” accounts on HP-UX Non-Truste systems.

Reconciliation
You can select "Is No Password Account?" on the account form. The adapter reconciles the value for the account as TRUE. If it is not selected, the adapter reconciles the value for the account as FALSE.

This table lists possible outcomes for "No Password" accounts during a modify operation when either:
- A password is provided.
- The value of the "Is No Password Account?" attribute is not sent in the request.

<table>
<thead>
<tr>
<th>Table 9. No Password Account possible outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>Null</td>
</tr>
<tr>
<td>Not null</td>
</tr>
<tr>
<td>Np Account 1/TRUE Unchanged</td>
</tr>
<tr>
<td>Replace</td>
</tr>
<tr>
<td>Np Account 0/False Unchanged</td>
</tr>
<tr>
<td>Replace</td>
</tr>
</tbody>
</table>

Chapter 5. First steps after installation  37
Table 9. No Password Account possible outcomes (continued)

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>It is already an Np Account</td>
<td>Request to make Np Account (that is from 0 to 1).</td>
<td>Not an Np account.</td>
<td>Request to make Np Account from Np Account (that is from 1 to 0).</td>
<td>It is already an Np Account</td>
<td>Request to make Np Account (that is from 0 to 1).</td>
<td>Not an Np account.</td>
<td>Request to make password Account from Np Account (that is from 1 to 0).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work Flow</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PASSWORD IS PRESENT</td>
<td>Fail the request as it is requesting for password change on Np Account.</td>
<td>Set Np Account. Do not set the password.</td>
<td>Set Password for the account.</td>
<td>Set as Password account by setting the password.</td>
<td>Do other modify operations.</td>
<td>Set Np Account.</td>
<td>Do other modify operations.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>UI without the Password field</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PASSWORD IS PRESENT</td>
<td>Fail the request as it is requesting for password change on Np Account.</td>
<td>N.A. The Password and Np Account value cannot come together.</td>
<td>Set Password for the account.</td>
<td>WARNING: Cannot set as password account. - No means to get the password here.</td>
<td>Do other modify operations.</td>
<td>Set Np Account.</td>
<td>Do other modify operations.</td>
<td></td>
</tr>
<tr>
<td>PASSWORD NOT PRESENT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Password management for account restoration

When an account is restored from being previously suspended, you are prompted to supply a new password for the reinstated account.

However, in some cases you might not want to be prompted for a password. The password requirement to restore an account falls into two categories: allowed and required.

How each restore action interacts with its corresponding managed resource depends on either the managed resource, or the business processes that you implement. Certain resources reject a password when a request is made to restore an account. In this case, you can configure IBM Security Identity Manager to forego the new password requirement. You can set the adapter to require a new password if your company requires that passwords are reset when accounts are restored.

The adapter profile JAR file contains a service.def file. In the service.def file, you can define whether a password is required as a new protocol option. When you import the adapter profile, if an option is not specified, the adapter profile importer determines the correct restoration password behavior from the schema.dsm1 file. Adapter profile components enable remote services to determine whether you discard a password that the user entered while multiple accounts on disparate resources are being restored. In this scenario, only some of the accounts that are being restored might require a password. Remote services discard the password from the restore action for those managed resources that do not require them.

Edit the <properties>...</properties> section of the service.def file to add the new protocol options, for example:

```xml
<property name = "com.ibm.itim.remoteservices.ResourceProperties.PASSWORD_NOT_REQUIRED_ON_RESTORE"><value>true</value>
</property>
<property name = "com.ibm.itim.remoteservices.ResourceProperties.PASSWORD_NOT_ALLOWED_ON_RESTORE"><value>false</value>
</property>
```
By adding the two options in the preceding example, you are ensuring that you are not prompted for a password when an account is restored.

**Note:** Before you set the property `PASSWORD_NOT_REQUIRED_ON_RESTORE` to `true`, ensure that the operating system supports restoring of an account without a password.

---

### Language pack installation

The adapters use a separate language package from the IBM Security Identity Manager.

See the IBM Security Identity Manager library and search for information about installing the adapter language pack.

---

### Verifying that the adapter is working correctly

After you install and configure the adapter, take steps to verify that the installation and configuration are correct.

**Procedure**

1. Test the connection for the service that you created on IBM Security Identity Manager.
2. Run a full reconciliation from IBM Security Identity Manager.
3. Run all supported operations such as add, modify, and delete on one user account.
4. Verify the `ibmdi.log` file after each operation to ensure that no errors are reported.
5. Verify the IBM Security Identity Manager log file `trace.log` to ensure that no errors are reported when you run an adapter operation.
Chapter 6. Adapter error troubleshooting

Troubleshooting can help you determine why a product does not function properly.

Use the following information and techniques to identify and resolve problems with the adapter. There is also information about troubleshooting errors that might occur during the adapter installation.

Techniques for troubleshooting problems

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem. Certain common techniques can help with the task of troubleshooting.

The first step in the troubleshooting process is to describe the problem completely. Problem descriptions help you and the IBM technical-support representative know where to start to find the cause of the problem. This step includes asking yourself basic questions:

• What are the symptoms of the problem?
• Where does the problem occur?
• When does the problem occur?
• Under which conditions does the problem occur?
• Can the problem be reproduced?

The answers to these questions typically lead to a good description of the problem, which can then lead you to a problem resolution.

What are the symptoms of the problem?

When you start to describe a problem, the most obvious question is “What is the problem?” This question might seem straightforward; however, you can break it down into several more-focused questions that create a more descriptive picture of the problem. These questions can include:

• Who, or what, is reporting the problem?
• What are the error codes and messages?
• How does the system fail? For example, is it a loop, hang, crash, performance degradation, or incorrect result?

Where does the problem occur?

Determining where the problem originates is not always easy, but it is one of the most important steps in resolving a problem. Many layers of technology can exist between the reporting and failing components. Networks, disks, and drivers are only a few of the components to consider when you are investigating problems.

The following questions help you to focus on where the problem occurs to isolate the problem layer:

• Is the problem specific to one operating system, or is it common across multiple operating systems?
• Is the current environment and configuration supported?
• Do all users have the problem?
• (For multi-site installations.) Do all sites have the problem?

If one layer reports the problem, the problem does not necessarily originate in that layer. Part of identifying where a problem originates is understanding the environment in which it exists. Take some time to completely describe the problem environment, including the operating system and version, all corresponding software and versions, and hardware information. Confirm that you are running within an environment that is a supported configuration. Many problems can be traced back to incompatible levels of software that are not intended to run together or are not fully tested together.

**When does the problem occur?**

Develop a detailed timeline of events that lead up to a failure, especially for those cases that are one-time occurrences. You can most easily develop a timeline by working backward: Start at the time an error was reported (as precisely as possible, even down to the millisecond), and work backward through the available logs and information. Typically, you must look only as far as the first suspicious event that you find in a diagnostic log.

To develop a detailed timeline of events, answer these questions:
• Does the problem happen only at a certain time of day or night?
• How often does the problem happen?
• What sequence of events leads up to the time that the problem is reported?
• Does the problem happen after an environment change, such as upgrading or installing software or hardware?

Responding to these types of questions can give you a frame of reference in which to investigate the problem.

**Under which conditions does the problem occur?**

Knowing which systems and applications are running at the time that a problem occurs is an important part of troubleshooting. These questions about your environment can help you to identify the root cause of the problem:
• Does the problem always occur when the same task is being done?
• Does a certain sequence of events happen for the problem to occur?
• Do any other applications fail at the same time?

Answering these types of questions can help you explain the environment in which the problem occurs and correlate any dependencies. Just because multiple problems might occur around the same time. However, the problems are not necessarily related.

**Can the problem be reproduced?**

From a troubleshooting standpoint, the ideal problem is one that can be reproduced. Typically, when a problem can be reproduced you have a larger set of tools or procedures at your disposal to help you investigate. Problems that you can reproduce are often easier to debug and solve.

However, problems that you can reproduce can have a disadvantage: If the problem is of significant business impact, you do not want it to recur. If possible,
re-create the problem in a test or development environment, which typically offers you more flexibility and control during your investigation.

- Can the problem be re-created on a test system?
- Do multiple users or applications encounter the same type of problem?
- Can the problem be re-created by running a single command, a set of commands, or a particular application?

For information about obtaining support, see Appendix F, “Support information,” on page 99.

**Warning and error messages**

A warning or error might be displayed in the user interface. The message provides information that the user must know about the adapter or when an error occurs.

Table 10 contains warnings or errors that might be displayed on the user interface if the adapter is installed on your workstation.

<table>
<thead>
<tr>
<th>Warning or error message</th>
<th>Corrective action</th>
</tr>
</thead>
<tbody>
<tr>
<td>The following error occurred - <em>Error Description.</em></td>
<td>IBM Security Identity Manager cannot establish a connection with IBM Tivoli Directory Integrator. To fix this problem, ensure that:</td>
</tr>
<tr>
<td></td>
<td>- Tivoli Directory Integrator is running</td>
</tr>
<tr>
<td></td>
<td>- The URL specified on the service form for IBM Tivoli Directory Integrator is correct</td>
</tr>
<tr>
<td>The login credential is missing or incorrect.</td>
<td>You must provide correct information for the adapter to function properly. To fix this problem, ensure that:</td>
</tr>
<tr>
<td></td>
<td>- The managed resource is functioning properly and that you are connected to the correct resource</td>
</tr>
<tr>
<td></td>
<td>- The Managed Resource Location that is specified on the service form is correct</td>
</tr>
<tr>
<td></td>
<td>- The administrator ID specified on the service form is correct</td>
</tr>
<tr>
<td></td>
<td>- The administrator password that is specified on the service form is correct</td>
</tr>
<tr>
<td></td>
<td>- SSH is enabled and running on the managed resource</td>
</tr>
<tr>
<td>The account exists.</td>
<td>The user is already added to the resource. This error might occur if you are attempting to add a user to the managed resource and IBM Security Identity Manager is not synchronized with the resource. To fix this problem, schedule a reconciliation between IBM Security Identity Manager and the resource. See the online help for information about scheduling a reconciliation.</td>
</tr>
<tr>
<td>The adapter does not have permission to add an account.</td>
<td>The administrator ID specified on the service form does not have permissions to add, modify, or delete the account. To fix this problem, do one of these steps:</td>
</tr>
<tr>
<td>The adapter does not have permission to modify an account.</td>
<td>- Assign the correct privileges to the current administrator ID</td>
</tr>
<tr>
<td>The adapter does not have permission to delete an account.</td>
<td>- Change the administrator ID to an administrator ID that has the correct privileges.</td>
</tr>
</tbody>
</table>
Table 10. Warning and error messages (continued)

<table>
<thead>
<tr>
<th>Warning or error message</th>
<th>Corrective action</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The required attributes are missing from the request.</td>
<td>One or more required attributes were not provided when you attempted to add, modify, delete, or search for a user. Type the required attributes for each field and try the action again.</td>
</tr>
<tr>
<td>• There were no attributes that were passed to the adapter in the request.</td>
<td></td>
</tr>
<tr>
<td>• One or more required attributes are missing in the request.</td>
<td></td>
</tr>
<tr>
<td>• A system error occurred adding an account. The account was not added.</td>
<td>This error might occur for several reasons. To fix this problem, ensure that:</td>
</tr>
<tr>
<td>• A system error occurred modifying an account. The account was not changed.</td>
<td>• The administrator ID specified on the service form is correct.</td>
</tr>
<tr>
<td>• A system error occurred deleting an account. The account was not deleted.</td>
<td>• The administrator password that is specified on the service form is correct.</td>
</tr>
<tr>
<td>• The search failed because of a system error.</td>
<td>• The administrator ID has the correct privileges to add, modify, or delete a user account.</td>
</tr>
<tr>
<td></td>
<td>• The network connection is not slow between IBM Security Identity Manager and IDI or IDI and the managed resource.</td>
</tr>
<tr>
<td>CTGIMT022E The search failed because of a system error: Error running script with Failed value:126</td>
<td>Verify that the sudo user configuration file does not contain syntax errors.</td>
</tr>
<tr>
<td>• The account was added but some attributes failed.</td>
<td>The account was created, modified, or deleted, but some of the specified attributes in the request were not set. See the list of attributes that failed and the error message that explains why the attribute failed. Correct the errors that are associated with each attribute and try the action again.</td>
</tr>
<tr>
<td>• The account was modified but some attributes failed.</td>
<td>Note: Review the documentation for the operating system of the managed resource to determine the correct values for some attributes.</td>
</tr>
<tr>
<td>• The account was deleted successfully, but other steps failed.</td>
<td></td>
</tr>
<tr>
<td>• The user cannot be modified because it does not exist.</td>
<td>This error might occur when you attempt to modify or delete a user. This error might also occur if you attempt to change the password for a user. To fix the problem, ensure that:</td>
</tr>
<tr>
<td>• An error occurred deleting the account because the account does not exist.</td>
<td>• The location that is specified for the managed resource is correct.</td>
</tr>
<tr>
<td></td>
<td>• The user was created on the resource.</td>
</tr>
<tr>
<td></td>
<td>• The user was not deleted from the resource.</td>
</tr>
<tr>
<td></td>
<td>If the user does not exist on the resource, create the user on the resource and then schedule a reconciliation. See the online help for information about scheduling a reconciliation.</td>
</tr>
<tr>
<td>• Search filter error.</td>
<td>The filter that is specified in the search request is not correct. Specify the correct filter and try the search action again.</td>
</tr>
<tr>
<td>• Invalid search filter.</td>
<td></td>
</tr>
<tr>
<td>The account is already suspended.</td>
<td>This error might occur if you attempt to suspend an account that was already suspended.</td>
</tr>
<tr>
<td>Warning or error message</td>
<td>Corrective action</td>
</tr>
<tr>
<td>------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| The account was not suspended.                                   | The request failed to suspend the account. To fix this problem, ensure that:  
  - The specified administrator ID is correct.  
  - The specified administrator password is correct.  
  - The administrator has the necessary privileges to suspend an account.  
  - The user exists on the specified managed resource.  
  See the `ibmdi.log` file in the solutions directory of the IBM Tivoli Directory Integrator for specific details about the error. |
| The account is already restored.                                 | This error might occur if you attempt to restore an account that was already restored.                                                                                                                                 |
| The account was not restored.                                    | The request failed to restore the account. To fix this problem, ensure that:  
  - The specified administrator ID is correct.  
  - The specified administrator password is correct.  
  - The administrator has the necessary privileges to restore an account.  
  - The user exists on the specified managed resource.  
  See the `ibmdi.log` file in the solutions directory of the IBM Tivoli Directory Integrator for specific details about the error. |
| The reconciliation is successful, but no accounts were added to your service. | On the service form, check or clear the **Use a Shadow File** check box.  
  - Check the IDI log to ensure that there is no mismatch for shadow file usage. |
| The application cannot establish a connection to *hostname*.     | Ensure that SSH is enabled on the managed resource and that the managed resource is operational and attached to the network.                                                                 |
Table 10. Warning and error messages (continued)

<table>
<thead>
<tr>
<th>Warning or error message</th>
<th>Corrective action</th>
</tr>
</thead>
</table>
| An error occurred creating, modifying, or deleting the Group name group. The application cannot establish a connection to managed resource. | Ensure that these conditions are true.  
- The name in the Administrator name field on the service form is specified correctly.  
- The value of the Password attribute on the service form is specified correctly.  
- The managed resource is operational and connected to the network. |

The IBM Tivoli Directory Integrator detected the following error. Error: Connector parameter `executeUserProfile` has a value that is not valid: `true`. | Clear the **Execute user profile?** check box for the service that is used in the operation. |

Sudo message: `sudo: sorry, you must have a tty to run sudo` | Comment out the line `Defaults requiretty` in the `sudoexec` file. |

---

**Solving adapter installation and operational problems**

You can obtain information that might be helpful in troubleshooting adapter installation and operational problems.

**About this task**

The term "adapter user name" is used throughout this procedure. The "adapter user name" is the UNIX account that is supplied on the IBM Security Identity Manager service form for the administrator name. This account is the account that is used by the adapter to open a connection to the target workstation.

**Note:** The following steps are written for the AIX operating system and must be updated with correct commands for other UNIX or Linux operating systems.

**Procedure**

1. Set log level to **Debug**. See the *IBM Security Dispatcher Installation and Configuration Guide*. If possible, get only the log file with the failed request.
2. Get the software versions from the log files. Perform the following searches:
   
   **Table 11. Search strings for software versions**

<table>
<thead>
<tr>
<th>Software</th>
<th>Log file search string</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dispatcher</td>
<td>RMI DispatcherImpl: Starting</td>
</tr>
<tr>
<td>Assembly line</td>
<td>UNIX/Linux Adapter AL version</td>
</tr>
<tr>
<td>Posix connector</td>
<td>Loaded com.ibm.di.connector.osconnector.PosixConnector</td>
</tr>
<tr>
<td>RXA library</td>
<td>RXA Version</td>
</tr>
</tbody>
</table>

3. Get the operating system version. On an AIX workstation issue the commands:
   ```
   % instfix -i | grep AIX_ML
   % oslevel -q -s
   ```

4. Ensure that OpenSSH version 4.7 or later is installed. Other versions of OpenSSH might function properly with this adapter, however if an issue is traced to OpenSSH, you might need to update your OpenSSH version to get support.

5. For OpenSSH configuration issues, do the following steps:
a. Ensure that the UsePrivilegeSeparation attribute is set to yes in the sshd_config file. The default value of UsePrivilegeSeparation is yes. If set to no the adapter account is locked.

b. Ensure that the ClientAliveInterval attribute in the sshd_config file is either commented out or set to 0. The default value of ClientAliveInterval is 0.

6. On a remote workstation, issue the following ssh commands and capture the results.
   % ssh username@ip-address "ssh -V"

   If sudo is used, issue these commands:
   % ssh username@ip-address "sudo ls /tmp"
   % ssh username@ip-address "which sudo"

   The username is the adapter user name. The ip-address is the IP address of the UNIX system that is being managed.

7. For reconciliation issues, do the following steps:
   a. Copy the AIXPConnRes.sh reconciliation file from the adapter solution directory to the AIX /tmp directory.
   b. Log in to the AIX system with the "adapter user name".
   c. Change the directory to the /tmp directory.
   d. Ensure that you have execute permission on the AIXPConnRes.sh file, chmod 777 AIXPConnRes.sh.
   e. Run the following command and save the recon.out file:
      AIXPConnRes.sh "grep -e :" true > recon.out 2>&1

      For Linux systems, depending on the command that is specified on the service form for the Command used to query failed logins field, use one of these commands:
      LinuxPConnRes.sh "grep -e :" true : "faillog -u %USER%"
      LinuxPConnRes.sh "grep -e :" true : "faillock --user %USER%"
      LinuxPConnRes.sh "grep -e :" true : "pam_tally2 --user %USER%"

      If sudo is not used, replace the value true with false. False is the value for the root user.

      All reconciliation files are in the adapter solution directory. The following table lists the names of the reconciliation files for various operating systems.

Table 12. Reconciliation file names

<table>
<thead>
<tr>
<th>Platform</th>
<th>Reconciliation file name</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX file system</td>
<td>AIXPConnRes.sh</td>
</tr>
<tr>
<td>HPUX not trusted</td>
<td>HPNTrustPConnRes.sh</td>
</tr>
<tr>
<td>HPUX trusted</td>
<td>HPTrustPConnRes.sh</td>
</tr>
<tr>
<td>Linux no shadow</td>
<td>LinuxPConnRes.sh</td>
</tr>
<tr>
<td>Linux with shadow</td>
<td>LinuxShadowPConnRes.sh</td>
</tr>
<tr>
<td>Solaris</td>
<td>SolarisPConnRes.sh</td>
</tr>
</tbody>
</table>

8. For sudo issues, do the following steps:
   a. Verify sudo setup per installation guide. See Appendix C, “Super user creation on a supported operating system,” on page 73.
b. Use the adapter user name to log in to the target system.
c. Use sudo to do manual commands on the target system. For example,
   
   ```
   sudo mkuser test1
   sudo passwd test1
   sudo rmuser test1
   ```

9. For ssh issues, use `ssh` and `sudo` to do manual commands on the target system. For example, log in to a system that has connectivity to the target system and issue the commands:

   **For sudo users**
   
   ```
   ssh user@target "sudo mkuser test1"
   ssh user@target "sudo passwd test1"
   ssh user@target "sudo rmuser test1"
   ```

   **For nonsudo users**
   
   ```
   ssh user@target "mkuser test1"
   ssh user@target "passwd test1"
   ssh user@target "rmuser test1"
   ```

---

**Known adapter issues**

You can use information about permissions, passwords, and other data to correct known issues with the adapter.

**/tmp directory permissions**

The permissions for the `/tmp` directory on the managed resource must be set to 777 to do the reconciliation operation by using the sudo user.

**Home directory permissions**

The adapter requires home directory permissions that are set to 755 to set the umask value.

The sudo user must have permissions on the home directory of the user whose umask value is added or changed. Otherwise, the adapter might not work as expected.

**HP-UX password age issues**

The password age attributes have certain restrictions for HP-UX Trusted and Non- Trusted systems.

The HP-UX Non- Trusted operating system sets password `MAX_AGE` and `MIN_AGE` to -1 during account creation if no values are supplied. However, on a modify operation, the operating system does not allow -1 for password `MIN_AGE`. The adapter account form is modified with a constraint on password `MIN_AGE` that prevents the user from entering a value less than 0.

The HP-UX Trusted operating system sets password `MAX_AGE` and `MIN_AGE` to 0 during account creation if no values are supplied. The operating system does not allow -1 for password `MIN_AGE` and `MAX_AGE`. The adapter account form is modified with a constraint on password `MIN_AGE` that prevents the user from entering a value less than 0. No constraint exists on password `MAX_AGE` because it can be -1 for HP-UX_Non- Trusted operating systems.

The following attributes cannot be managed on HP-UX Non- Trusted systems:

   - `password warning age`
maximum number of days the account can remain valid after the password expires. For AIX systems the duration is specified in weeks.

number of days the account can remain idle

allowed number of login retries before locking the account

account expiration date

**No support for adding the primary group of a user to the secondary groupset of the user**

SUSE Linux and Solaris operating systems do not support adding the primary group of a user to the secondary groupset of the user.

The UNIX and Linux Adapter cannot support a function that is not supported by the operating system. If you attempt to add the primary group to the secondary groupset of the user, the operation fails on SUSE Linux and Solaris systems. Although the primary group is not added, no error message is returned. The command that is used for this function does not generate an error message.
Chapter 7. Adapter upgrade

Upgrading the adapter involves tasks such as upgrading the connector, dispatcher, and the existing adapter profile.

To verify the required version of these adapter components, see the adapter release notes.

Connector upgrade

The new adapter package might require you to upgrade the connector.

Before you upgrade the connector, verify the version of the connector.

• If the connector version mentioned in the release notes is later than the existing version on your workstation, install the connector.
• If the connector version mentioned in the release notes is the same or earlier than the existing version, do not install the connector.

Note: Stop the dispatcher service before the upgrading the connector and start it again after the upgrade is complete.

Dispatcher upgrade

The new adapter package might require you to upgrade the Dispatcher.

Before you upgrade the dispatcher, verify the version of the dispatcher.

• If the dispatcher version mentioned in the release notes is later than the existing version on your workstation, install the dispatcher.
• If the dispatcher version mentioned in the release notes is the same or earlier than the existing version, do not install the dispatcher.

Note: Stop the dispatcher service before the upgrading the dispatcher and start it again after the upgrade is complete.

Upgrade of an existing adapter profile

Read the adapter release notes for any specific instructions before you import a new adapter profile on IBM Security Identity Manager.

See "Importing the adapter profile into the IBM Security Identity Manager server" on page 11.

Note: Restart the dispatcher service after you import the profile. Restarting the dispatcher clears the assembly lines cache and ensures that the dispatcher runs the assembly lines from the updated adapter profile.
Chapter 8. Adapter uninstallation

You can uninstall the UNIX and Linux Adapter completely.

- Uninstall the adapter from the IBM Tivoli Directory Integrator server.
- Remove the adapter profile from the IBM Security Identity Manager server.

Uninstalling the adapter from the Tivoli Directory Integrator server

When the adapter is installed, the JAR file that is required for uninstalling the adapter is created in the $ITDI_HOME/PosixAdapterUninstall directory.

Procedure

1. Stop the adapter service. See “Adapter service start, stop, and restart” on page 11.
2. Run the PosixAdapterUninstall.jar file from PosixAdapterUninstall directory.
   If you run the command from a different directory, you must specify the full file path to the uninstaller.jar file.
   $TDI_HOME/jvm/jre/bin/java -jar uninstaller.jar

Adapter profile removal from the IBM Security Identity Manager server

Before you remove the adapter profile, ensure that no objects exist on your IBM Security Identity Manager server that reference the adapter profile.

Examples of objects on the IBM Security Identity Manager server that can reference the adapter profile are:

- Adapter service instances
- Policies referencing an adapter instance or the profile
- Accounts

For specific information about removing the adapter profile, see the IBM Security Identity Manager product documentation.
Chapter 9. Adapter reinstallation

There are no special considerations for reinstalling the adapter. You are not required to remove the adapter before reinstalling.

For more information, see Chapter 7, “Adapter upgrade,” on page 51.
Appendix A. Adapter attributes

The IBM Security Identity Manager server communicates with the adapter by using attributes that are included in transmission packets that are sent over a network.

The combination of attributes, depends on the type of action that the IBM Security Identity Manager server requests from the adapter.

Table 13. Account form attributes, descriptions, permissions, and applicable operating systems

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Permissions</th>
<th>Operating systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>erUid</td>
<td>Specifies the login name and user name.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td>erPosixUid</td>
<td>Specifies the user ID.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td>erPosixDupUid</td>
<td>Specifies that a non-unique ID can be assigned to the user.</td>
<td>Write</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td>erPosixSudoersPath</td>
<td>Specifies the path to the sudoers file on the resource.</td>
<td>Write</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Permissions</td>
<td>Operating systems</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------------------------------------</td>
<td>-----------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>erPosixSudoPrivileges</td>
<td>Specifies the sudo privileges for the user or group that is associated with the account.</td>
<td>Read</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td>erPosixReturnSudoPrivileges</td>
<td>Specifies whether to return sudo privileges during account reconciliation.</td>
<td>Write</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td>erPassword</td>
<td>Specifies the password for the account.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td>erPosixForcePwdChange</td>
<td>Specifies whether the user is required to change the login password upon next login.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td>erPosixMaxPwdAge</td>
<td>Specifies the maximum age for a password.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Permissions</td>
<td>Operating systems</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>erPosixMinPwdAge</td>
<td>Specifies the minimum age for a password.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td>erPosixPwdMaxRepeats</td>
<td>Specifies the maximum repeated characters that are allowed in a password.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td>erPosixPwdWarnAge</td>
<td>Specifies the age of a password before a message that warns the user about password expiration is sent.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td>erPosixPwdLastChange</td>
<td>Specifies the date on which a password was last changed.</td>
<td>Read</td>
<td>Linux NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td>erPosixExpireDate</td>
<td>Specifies the date on which the account expires.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td>erPosixIdleDays</td>
<td>Specifies the number of days the account can remain idle before the account is suspended.</td>
<td>Read and Write</td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td>erPosixGecos</td>
<td>Specifies a descriptive comment for the user account.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td>Note: The back quotation mark character (&quot;) is not allowed.</td>
<td></td>
<td>Linux NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Permissions</td>
<td>Operating systems</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>erPosixPrimaryGroup</td>
<td>Specifies the primary group for the user.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td>erPosixSecondaryGroup</td>
<td>Specifies the secondary groups for the user.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td>erPosixHomeDir</td>
<td>Specifies the home directory for the user.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td>erPosixDefaultHomeDir</td>
<td>Specifies to create a home directory while the account is created. This</td>
<td>Read and Write</td>
<td>Linux NonShadow</td>
</tr>
<tr>
<td></td>
<td>attribute does not apply to RHEL.</td>
<td></td>
<td>Linux Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td>erPosixNPAccount</td>
<td>Specifies that the account has no password.</td>
<td>Read and Write</td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td>erPosixPerHomeDir</td>
<td>Specifies the permissions for the home directory.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Permissions</td>
<td>Operating systems</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------</td>
</tr>
<tr>
<td><code>erPosixShell</code></td>
<td>Specifies the login shell of the user.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td><code>erPosixUmask</code></td>
<td>Specifies the umask.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td><code>erPosixLastAccessDate</code></td>
<td>Specifies the date on which the account was last accessed.</td>
<td>Read</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td><code>erPosixAT</code></td>
<td>Specifies whether AT jobs are allowed.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td><code>erPosixCron</code></td>
<td>Specifies whether CRON jobs are allowed.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td><code>erPosixPwdMaxAge</code></td>
<td>Specifies the maximum amount of time that a password can be changed after the maximum password age.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
</tbody>
</table>

Appendix A. Adapter attributes  61
Table 13. Account form attributes, descriptions, permissions, and applicable operating systems (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Permissions</th>
<th>Operating systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>erPosixKillUserProcess</td>
<td>Specifies whether to end the user sessions when a suspend user request is processed.</td>
<td>Write</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td>erPosixCopyAdpFilesTo</td>
<td>Specifies an alternative directory location to store the adapter scripts. The default location is /tmp.</td>
<td>Write</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td>erPosixPreExec</td>
<td>Specifies a user-defined command to run before a resource request.</td>
<td>Write</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td>erPosixPreExecRunOption</td>
<td>Specifies to run a resource request only if a pre-exec command succeeds.</td>
<td>Write</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td>erPosixPostExec</td>
<td>Specifies a user-defined command to run after a resource request.</td>
<td>Write</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
</tbody>
</table>
### Table 13. Account form attributes, descriptions, permissions, and applicable operating systems (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Permissions</th>
<th>Operating systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>erPosixPostExecRunOption</td>
<td>Specifies to run a user-defined post-exec command only if the resource command succeeds.</td>
<td>Write</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td>erPosixAdminUser</td>
<td>Specifies whether the password belongs to an administrator.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixAuth1</td>
<td>Specifies the primary authorization methods for a user.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixAuth2</td>
<td>Specifies the secondary authorization methods for a user.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixDaemonAllowed</td>
<td>Specifies whether the user is allowed to run daemon processes.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixLoginRetries</td>
<td>Specifies the maximum number of unsuccessful logins that are allowed before the account is locked.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Suse Linux</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td>erPosixSuGroup</td>
<td>Specifies the groups whose members can use the su command to switch to this user.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixAdmGroups</td>
<td>Specifies the groups for which the user is an administrator.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixRoles</td>
<td>Specifies the roles that the user is assigned.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixSuAllowed</td>
<td>Specifies whether another user can switch to this user with the su command.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixRLoginAllowed</td>
<td>Specifies whether the user is allowed to log in remotely with the telnet or rlogin commands.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixLoginAllowed</td>
<td>Specifies whether the user is allowed to log in to the system with the login command.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Permissions</td>
<td>Operating systems</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>erAccountStatus</td>
<td>Specifies the status of the account.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixAuditClasses</td>
<td>Specifies the list of audit classes for a user.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixSoftCore</td>
<td>Specifies the soft limit, any value less than the maximum, for the largest core file a user process can create.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixHardCore</td>
<td>Specifies the largest core file a user process can create.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixSoftCPU</td>
<td>Specifies the soft limit, any value less than the maximum, for the largest amount of system unit time a user process can use. The time is specified in seconds.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixHardCPU</td>
<td>Specifies the largest amount of system unit time a user process can use. The time is specified in seconds.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixSoftData</td>
<td>Specifies the soft limit, any value less than the maximum, for the largest data segment that a user process can contain.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixHardData</td>
<td>Specifies the limit for the largest data segment that a user process can contain.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixSoftFileSize</td>
<td>Specifies the soft limit, any value less than the maximum, for the largest file a user process can create.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixHardFileSize</td>
<td>Specifies the limit for the largest file a user process can create.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixLoginTimes</td>
<td>Specifies the days and times a user is allowed to log in.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixSoftStack</td>
<td>Specifies the soft limit, any value less than the maximum, for the largest stack segment for a user process.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixHardStack</td>
<td>Specifies the limit for the largest stack segment for a user process.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Permissions</td>
<td>Operating systems</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>erPosixTrustedPath</td>
<td>Specifies the trusted path status of the user.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixAuthGrammar</td>
<td>Specifies the user authentication method.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixPwdMinAlphaChar</td>
<td>Specifies the minimum number of alphabetic characters in a password.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixPwdMinOtherChar</td>
<td>Specifies the minimum number of non-alphabetic characters in a password.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixPwdMinDiff</td>
<td>Specifies the minimum difference in characters that are allowed between passwords.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixPwdMinLen</td>
<td>Specifies the minimum length for a password.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixPwdCheck</td>
<td>Specifies whether to check the password in a dictionary.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixPwdDiction</td>
<td>Specifies the dictionary files to check for the password.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixPwdHistory</td>
<td>Specifies the number of passwords to be remembered before reuse.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixPwdHistoryExpire</td>
<td>Specifies the number of weeks that must pass before the password history is erased.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixValidTtys</td>
<td>Specifies the terminal types through which the user can log in.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixRegistry</td>
<td>Specifies the registry to be used for authentication.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixSoftRss</td>
<td>Specifies the soft limit, any value less than the maximum, for the largest amount of physical memory that can be allocated by a user process. This limit is not enforced by the system.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixHardRss</td>
<td>Specifies the largest amount of physical memory that can be allocated by a user process. This limit is not enforced by the system.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
</tbody>
</table>
Table 13. Account form attributes, descriptions, permissions, and applicable operating systems (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Permissions</th>
<th>Operating systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>erPosixSoftNoFiles</td>
<td>Specifies the soft limit, any value less than the maximum, for the number of file descriptors a user process can have open at one time.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixHardNoFiles</td>
<td>Specifies the maximum number of file descriptors a user process can have open at one time.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixHostsAllowedLogin</td>
<td>Specifies the workstations to which a user can log in.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixHostsDeniedLogin</td>
<td>Specifies the workstations to which a user cannot log in.</td>
<td>Read and Write</td>
<td>AIX</td>
</tr>
<tr>
<td>erPosixDelUserInUse</td>
<td>Specifies whether to end the user processes when a delete account request is processed.</td>
<td>Read and Write</td>
<td>Linux NonShadow Linux Shadow</td>
</tr>
</tbody>
</table>

Group form attributes

The IBM Security Identity Manager server communicates with the adapter for group management by using specific attributes.

Table 14 lists the attributes that are used by the adapter. The table also gives the permissions that are needed for the attribute.

Table 14. Group form attributes

<table>
<thead>
<tr>
<th>Attribute name on the UNIX and Linux operating systems group form on IBM Security Identity Manager</th>
<th>Permissions</th>
<th>Supported operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group name</td>
<td>Read and Write</td>
<td>✓</td>
</tr>
<tr>
<td>Group ID number</td>
<td>Read and Write</td>
<td>✓</td>
</tr>
<tr>
<td>Administrator group</td>
<td>Read and Write</td>
<td>✓</td>
</tr>
<tr>
<td>Group administrators</td>
<td>Read and Write</td>
<td>✓</td>
</tr>
<tr>
<td>Group projects</td>
<td>Read and Write</td>
<td>✓</td>
</tr>
<tr>
<td>Allow duplicate group IDs</td>
<td>Write</td>
<td>✓</td>
</tr>
<tr>
<td>Sudo privileges</td>
<td>Read</td>
<td>✓</td>
</tr>
</tbody>
</table>

Attributes by UNIX and Linux Adapter actions

Typical adapter actions can be listed by their functional transaction group.

The following lists include more information about required and optional attributes that are sent to the adapter to complete that action.
System Login Add

A System Login Add is a request to create a user account with the specified attributes.

Table 15. Add request attributes for AIX, HPUX, Linux, and Solaris

<table>
<thead>
<tr>
<th>Required attribute</th>
<th>Optional attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>erUid</td>
<td>All other supported attributes</td>
</tr>
</tbody>
</table>

System Login Change

A System Login Change is a request to change one or more attributes for the specified users.

Table 16. Change request attributes for AIX, HPUX, Linux, and Solaris

<table>
<thead>
<tr>
<th>Required attribute</th>
<th>Optional attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>erUid</td>
<td>All other supported attributes</td>
</tr>
</tbody>
</table>

System Login Delete

A System Login Delete is a request to remove the specified user from the directory.

Table 17. Delete request attributes for AIX and Solaris

<table>
<thead>
<tr>
<th>Required attribute</th>
<th>Optional attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>erUid</td>
<td>erPosixHomeDirRemove</td>
</tr>
</tbody>
</table>

Table 18. Delete request attributes for HPUX and Linux

<table>
<thead>
<tr>
<th>Required attribute</th>
<th>Optional attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>erUid</td>
<td>erPosixHomeDirRemove</td>
</tr>
<tr>
<td></td>
<td>erPosixUseShadow</td>
</tr>
</tbody>
</table>

System Login Suspend

A System Login Suspend is a request to disable a user account. The user is not removed and the account attributes are not modified.

Table 19. Suspend request attributes for AIX and Solaris

<table>
<thead>
<tr>
<th>Required attribute</th>
<th>Optional attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>erUid</td>
<td>erPosixHomeDirRemove</td>
</tr>
<tr>
<td>erAccountStatus</td>
<td>erPosixKillUserProcess</td>
</tr>
</tbody>
</table>

Table 20. Suspend request attributes for HP-UX and Linux

<table>
<thead>
<tr>
<th>Required attribute</th>
<th>Optional attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>erUid</td>
<td>erPosixHomeDirRemove</td>
</tr>
<tr>
<td>erAccountStatus</td>
<td>erPosixUseShadow</td>
</tr>
<tr>
<td></td>
<td>erPosixKillUserProcess</td>
</tr>
</tbody>
</table>
System Login Restore

A System Login Restore is a request to activate a user account that was previously suspended. After an account is restored, the user can access the system with the same attributes as the ones before the Suspend function was called.

Table 21. Restore request attributes for AIX

<table>
<thead>
<tr>
<th>Required attribute</th>
<th>Optional attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>erUid</td>
<td>erPosixHomeDirRemove</td>
</tr>
<tr>
<td>erAccountStatus</td>
<td></td>
</tr>
</tbody>
</table>

Table 22. Restore request attributes for Solaris

<table>
<thead>
<tr>
<th>Required attribute</th>
<th>Optional attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>erUid</td>
<td>erPosixHomeDirRemove</td>
</tr>
<tr>
<td>erAccountStatus</td>
<td></td>
</tr>
<tr>
<td>erPassword</td>
<td></td>
</tr>
</tbody>
</table>

Test

No attributes are needed to test the connection to the managed resource.

The following table identifies attributes that are needed to test the connection.

Table 23. Test attributes

<table>
<thead>
<tr>
<th>Required attribute</th>
<th>Optional attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

Reconciliation

The Reconciliation request synchronizes user account information between IBM Security Identity Manager and the managed resource.

Table 24. Reconciliation request attributes for AIX and Solaris

<table>
<thead>
<tr>
<th>Required attribute</th>
<th>Optional attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>erPosixHomeDirRemove</td>
</tr>
<tr>
<td></td>
<td>erPosixSudoersPath</td>
</tr>
<tr>
<td></td>
<td>erPosixReturnSudoPrivileges</td>
</tr>
</tbody>
</table>

Table 25. Reconciliation request attributes for HP-UX and Linux

<table>
<thead>
<tr>
<th>Required attribute</th>
<th>Optional attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>erPosixHomeDirRemove</td>
</tr>
<tr>
<td></td>
<td>erPosixUseShadow</td>
</tr>
<tr>
<td></td>
<td>erPosixSudoersPath</td>
</tr>
<tr>
<td></td>
<td>erPosixReturnSudoPrivileges</td>
</tr>
</tbody>
</table>
**Group add**

Group add is a request to create a group with the specified attribute.

<table>
<thead>
<tr>
<th>Required attribute</th>
<th>Optional attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>erPosixGroupName</code></td>
<td>All other supported attributes</td>
</tr>
</tbody>
</table>

**Group change**

Group change is a request to modify group attributes with the specified attribute.

<table>
<thead>
<tr>
<th>Required attribute</th>
<th>Optional attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>erPosixGroupName</code></td>
<td>All other supported attributes</td>
</tr>
</tbody>
</table>

**Group delete**

Group delete is a request to delete a group with the required `erPosixGroupName` attribute on the account form of the AIX, HPUX, Linux, and Solaris operating systems.
Appendix B. Adapter installation on a z/OS operating system

The Dispatcher must be installed before you install any adapter that is based on IBM Tivoli Directory Integrator, including the UNIX and Linux Adapter.

If not already installed, download the Dispatcher software package from your account in IBM Passport Advantage. The Dispatcher installation instructions are included in the package.

IBM Tivoli Directory Integrator POSIX connector installation

You must install the connector on the workstation where you want to install the adapter.

Procedure

1. Locate the delivered adapter compressed file.
2. Extract the contents of the compressed file into a temporary directory and navigate to that directory.
3. From the temporary directory, locate and navigate to the zSystem directory.
4. Under the zSystem directory, locate the following two files:
   - PosixAdapter.tar
   - instPosix_zOS.sh

   Note: The PosixAdapter.tar file is a binary UNIX tar file and the instPosix_zOS.sh file is a UNIX shell script.
5. Copy the two files to the same directory on a z/OS workstation where you want to install the adapter.
6. Run the following command to set the executable permissions for the instPosix_zOS.sh file:
   ```
   chmod +x instPosix_zOS.sh
   ```
7. Run the following command to begin the connection installation:
   ```
   ./ instPosix_zOS.sh
   ```

   The following dialog is displayed:
   
   ************************************************
   TDI POSIX Connector Installation Program
   ************************************************

   You will prompted to enter the following information:

   Your TDI solution directory.
   
   Make sure you have the above information available and
   and the PosixAdapter.jar is located in the current directory
   before you continue

   1. Install
   2. Quit

   Please enter choice: 1

   Enter the solution directory name (full path): /u/user2/rmi/soldir
Verifying the solution directory /u/user2/rmi/soldir...
Extracting content of PosixAdapter.jar...
Getting connector files from /u/user2/rmi/PosixAdapter...

Installation complete, press any key to continue.

Note: The path in the example might be different on your workstation.
Appendix C. Super user creation on a supported operating system

You can specify a super user instead of a root user to do administration tasks. To create a super user, follow the directions that are specified for your operating system.

Creating a super user on an AIX operating system

You can create a user with required permissions to run the adapter correctly on a workstation that uses an AIX operating system.

About this task

In this task, the user is "tdiuser".

Procedure

1. Create a user with security group permission.
   a. Issue the command:
      ```
      mkuser home="/home/tdiuser" pgrp="security" shell="/usr/bin/ksh" tdiuser
      ```
   b. Confirm the group information. Issue the command:
      ```
      bash-2.05b$ id tdiuser
      ```
      The system response is this message:
      ```
      uid=215(tdiuser) gid=7(security) groups=0(system)
      ```
   c. Set the following statement in the user PATH environment variable:
      ```
      PATH=/usr/bin:/etc:/usr/sbin:/usr/ucb:$HOME/bin:/usr/bin/X11:/sbin:
      /usr/local/bin
      ```
      The following commands must be in the user path:
      ```
      mv, tee, cp, kill, chsec, mkdir, rm, sudo
      ```
      If the super user is used to log in and run commands, then '.' can be added to the PATH environment variable.

2. Grant sudo permissions to the user for AIX commands.
   a. If the super user is used to log in and run commands, then '.' can be added to the PATH environment variable.
   b. Grant sudo permissions to the user for AIX commands.
      Note: By default, the sudo command requires user authentication before it runs a command. To modify this behavior, add the NOPASSWD tag to the sudoers file entry.
      a. Open the sudoers file. Issue the following command:
         ```
         bash-2.05b$ visudo
         ```
      b. If the line Defaults requiretty exists in the file, comment it out.
         ```
         #Defaults requiretty
         ```
      c. Insert the following lines to allow sudo access. The entry beginning with tdiuser must be entered on a single line. It is displayed here as multiple lines for readability.
         ```
         # User privilege specification
         tdiuser ALL=NOPASSWD:/usr/bin/pwdadm,/usr/bin/passwd,/usr/bin/mkuser,
         /usr/sbin/rmuser,/usr/bin/chuser,/usr/bin/chmod,/usr/bin/cat,
         /usr/bin/rm,/usr/bin/tee,/usr/bin/ed,/usr/bin/groups,/usr/bin/ls,
         /usr/bin/logins,/usr/sbin/lsuser,/usr/bin/mv,/usr/sbin/lsgroup,
         ```
The following commands are used by the connector but are not needed in the sudoers file. However, if the sudo user is used, the user needs execute permissions on these commands.

```
/usr/bin/tr, /usr/bin/cut, /usr/bin/egrep, /usr/bin/awk,
/usr/bin/sort, /usr/bin/ps, /usr/bin/sed
```

d. Validate the format of the `/etc/sudoers` file. Issue the command:

```
visudo -c
```

If syntax is wrong the command prompts an error message, for example:

```
$ visudo -c
>>> sudoers file: syntax error, line 30 <<<
parse error in /etc/sudoers near line 30
```

**Note:** The sudo access command paths that are listed here are an example. The actual command paths vary depending upon the resource. Ensure that the correct path is specified in the `sudoers` file.

3. Set the password for the newly created user. Issue the command:

```
bash-2.05b$ passwd tdiuser
```

---

**Creating a super user on a Linux operating system**

You can create a user with required permissions to run the adapter correctly on a workstation that uses a Linux operating system.

**About this task**

The adapter supports both SUSE and RHEL. In this example, the user is “tdiuser”.

**Procedure**

1. Create a user with security group permission.
   a. Issue the command:
      ```
      useradd -d "/home/tdiuser" -s "/bin/bash" -m tdiuser
      ```
   b. Set the following statement in the user PATH environment variable:
      ```
      PATH=/usr/bin:/usr/sbin:/etc:
      ```
      The following commands must be in the user path:
      ```
      mv, tee, cp, kill, mkdir, rm, faillog, faillock, pam_tally2, grep, lastlog, sudo
      ```
      **Note:** For SLES 11 and higher, the `faillog` command full path is
      `/usr/sbin/faillog`.
      If the super user is used to log in and run commands, then `'.'` can be added to the PATH environment variable.

2. Grant sudo permissions to the user for all commands.
   **Note:** By default, the `sudo` command requires user authentication before it runs a command. To modify this behavior, add the NOPASSWD tag to the `sudoers` file entry.
   a. Open the `sudoers` file. Issue the following command:
      ```
      bash-2.05b$ visudo
      ```
b. If the line `Defaults requiretty` exists in the file, comment it out.
   
   ```
   #Defaults requiretty
   ```

c. Insert the following lines to allow sudo access. The entry beginning with `tdiuser` must be entered on a single line. It is displayed here as multiple lines for readability.

   Modify the command paths to match your operating system. Update the user path if necessary.
   
   ```
   # User privilege specification
   tdiuser ALL=NOPASSWD:/usr/bin/passwd,/usr/sbin/useradd,
   /usr/sbin/usermod,/usr/sbin/userdel,/usr/bin/tee,/bin/chmod,
   /bin/cat,/bin/ls,/usr/bin/chage,/usr/bin/groups,/bin/ed,
   /bin/cp,/usr/bin/faillog,/usr/sbin/groupadd,/usr/sbin/groupmod,
   /usr/sbin/groupdel,/usr/bin/kill,/bin/hostname,/sbin/faillock,
   /sbin/pam_tally2,/bin/mkdir,/bin/rm,/usr/bin/lastlog
   ```

   The following commands are used by the connector but are not needed in the sudoers file. However, if the sudo user is used, the user needs execute permissions on these commands:

   `tr`, `cut`, `awk`, `sed`, `sort`, `grep`, `ps`

d. Validate the format of the `/etc/sudoers` file Issue the command:

   ```
   visudo -c
   ```

   If syntax is wrong the command prompts an error message, for example:

   ```
   $ visudo -c
   >>> sudoers file: syntax error, line 30 <<<
   parse error in /etc/sudoers near line 30
   ```

   **Note:** The sudo access command paths that are listed here are an example. The actual command paths vary depending upon the resource. Ensure that the correct path is specified in the sudoers file.

   For example, the complete path of `ed` command is `/bin/ed` for RHEL systems, `/usr/bin/ed` for SUSE systems, and `/bin/ed` for Debian systems.

3. Set the password for the newly created user. Issue the command:

   ```
   bash-2.05b$passwd tdiuser
   ```

---

**Creating a super user on a Solaris operating system**

You can create a user with the required permissions to run the adapter correctly on a workstation that uses a Solaris operating system.

**About this task**

In this example, the user is "tdiuser".

**Procedure**

1. Create a user and specify the home directory.

   a. Issue the command:

   ```
   useradd -d "/home/tdiuser" -s "/bin/sh" -m tdiuser
   ```

   b. Ensure that the `/home/tdiuser/.profile` file exists. If not, you must create the `.profile` file.

   c. Set the following statement in the user PATH environment variable:

   ```
   PATH=/usr/bin:/etc:/usr/local/sbin:/usr/local/bin
   ```

   The following commands must also be in the user path:
mv, tee, cp, kill, mkdir, rm, sudo

If the super user is used to log in and run commands, then `.' can be added to the PATH environment variable.

2. Grant sudo permissions to the user for all commands.

   **Note:** By default, the `sudo` command requires user authentication before it runs a command. To modify this behavior, add the NOPASSWD tag to the sudoers file entry.

   a. Open the sudoers file. Issue the following command:

      ```bash
      bash-2.05b$ visudo
      ```

   b. If the line `Defaults requiretty` exists in the file, comment it out:

      ```bash
      #Defaults requiretty
      ```

   c. Insert the following lines to allow sudo access. The entry beginning with `tdiuser` must be entered on a single line. It is displayed here as multiple lines for readability.

      ```bash
      # User privilege specification
      tdiuser ALL=NOPASSWD:/usr/bin/passwd,/usr/sbin/useradd, 
      /usr/sbin/usermod,/usr/sbin/userdel,/usr/bin/tee,/usr/bin/chmod, 
      /usr/bin/cat,/usr/bin/logins,/usr/bin/ls,/usr/bin/ed,/usr/bin/cp, 
      /usr/sbin/groupadd,/usr/sbin/groupmod,/usr/sbin/groupdel, 
      /usr/bin/mkdir,/usr/bin/rm,/usr/bin/kill,/usr/bin/hostname
      ```

      The following commands are used by the connector but are not needed in the sudoers file. However, if the sudo user is used, the user needs execute permissions on these commands.

      ```bash
      /usr/bin/tr, /usr/bin/cut, /usr/bin/egrep, /usr/bin/awk, 
      /usr/bin/sort, /usr/bin/ps, /usr/bin/sed
      ```

   d. Validate the format of the `/etc/sudoers` file. Issue the command:

      ```bash
      visudo -c
      ```

      If syntax is wrong the command prompts an error message, for example:

      ```bash
      $ visudo -c
      >>> sudoers file: syntax error, line 30 <<<
      parse error in /etc/sudoers near line 30
      ```

      **Note:** The sudo access command paths that are listed here are an example. The actual command paths vary depending upon the resource. Ensure that the correct path is specified in the sudoers file.

3. Set the password for the newly created user. Issue the command:

   ```bash
   bash-2.05b$ passwd tdiuser
   ```

---

**Creating a super user on an HP-UX Non-Trust operating system**

You can create a user with required permissions to run the adapter correctly on a workstation that uses an HP-UX Non-Trust operating system.

**About this task**

In this example, the user is "tdiuser".

**Procedure**

1. Create a user and specify the home directory.

   a. Issue the command:

      ```bash
      useradd -d "/home/tdiuser" -s "/sbin/sh" -m tdiuser
      ```
b. Ensure that the /home/tdiuser/.profile file exists. If not, you must create the .profile file.
c. Set the following statement in the user PATH environment variable:
   PATH=/usr/bin:/usr/sbin:/etc:/usr/local/bin:/usr/sam/bin:/usr/sbin/acct:
   The following commands must be in the user path:
   mv, tee, cp, kill, usermod.sam, mkdir, rm, fwtmp, sudo
   If the super user is used to log in and run commands, then '.' can be added to the PATH environment variable.

2. Grant sudo permissions to the user for all commands.

   **Note:** By default, the sudo command requires user authentication before it runs a command. To modify this behavior, add the NOPASSWD tag to the sudoers file entry.
   a. Open the sudoers file. Issue the following command:
      bash-2.05b$ visudo
   b. If the line Defaults requiretty exists in the file, comment it out.
      #Defaults requiretty
c. Insert the following lines to allow sudo access. The entry beginning with tdiuser must be entered on a single line. It is displayed here as multiple lines for readability.
      # User privilege specification
      tdiuser ALL=NOPASSWD:/usr/bin/chmod,/usr/bin/cat,/usr/sbin/logins,
      /usr/bin/ls,/usr/bin/passwd,/usr/sbin/useradd,/usr/sbin/usermod,
      /usr/sbin/userdel,/usr/bin/tee,/usr/bin/ed,/usr/sbin/groupadd,
      /usr/sbin/groupdel,/usr/sbin/groupmod,/usr/bin/cp,/usr/bin/mkdir,
      /usr/bin/rm,/usr/bin/kill,/usr/bin/hostname,/usr/sbin/acct/fwtmp,
      /usr/bin/test

      The following commands are used by the connector but are not needed in the sudoers file. However, if the sudo user is used, the user needs execute permissions on these commands.
      /usr/bin/tr, /usr/bin/cut, /usr/bin/egrep, /usr/bin/awk,
      /usr/bin/head, /usr/bin/sort, /usr/bin/ps, /usr/bin/sed
d. Validate the format of the /etc/sudoers file issue the command:
      visudo -c
      If syntax is wrong the command prompts an error message, for example:
      $ visudo -c
      >>> sudoers file: syntax error, line 30 <<<
      parse error in /etc/sudoers near line 30

      **Note:** The sudo access command paths that are listed here are an example. The actual command access paths vary depending upon the resource. Ensure that the correct path is specified in the sudoers file.

3. Set the password for the newly created user. Issue the command:
   bash-2.05b$ passwd tdiuser

---

**Creating a super user on an HP-UX Trusted operating system**

You can create a user with required permissions to run the adapter correctly on a workstation that uses an HP-UX Trusted operating system.
**About this task**

In this example, the user is "tdiuser".

**Procedure**

1. Create a user and specify the home directory.
   a. Issue the command:

```
useradd -d "/home/tdiuser" -s "/sbin/sh" -m tdiuser
```
   b. Ensure that the `/home/tdiuser/.profile` file exists. If not, you must create the `.profile` file.
   c. Set the following statement in the user PATH environment variable:

```
PATH=/usr/bin:/usr/sbin:/etc:/usr/local/bin:/usr/sam/lbin:/usr/sbin/acct:
```

The following commands must be in the user path:

- `mv`
- `tee`
- `cp`
- `kill`
- `usermod.sam`
- `mkdir`
- `rm`
- `fwtmp`
- `sudo`

If the super user is used to log in and run commands, then `:` can be added to the PATH environment variable.

2. Grant sudo permissions to the user for all commands.

   **Note:** By default, the `sudo` command requires user authentication before it runs a command. To modify this behavior, add the NOPASSWD tag to the sudoers file entry.
   a. Open the sudoers file. Issue the following command:

```
bash-2.05b$ visudo
```
   b. If the line `Defaults requiretty` exists in the file, comment it out.

```
#Defaults requiretty
```
   c. Insert the following lines to allow sudo access. The entry beginning with `tdiuser` must be entered on a single line. It is displayed here as multiple lines for readability.

```
# User privilege specification
tdiuser ALL=NOPASSWD:/usr/bin/passwd,/usr/sbin/useradd,
/usr/sbin/usermod,/usr/sbin/userdel,/usr/bin/cat,/usr/lbin/getprpw,
/usr/sbin/modprpw,/usr/bin/chmod,/usr/bin/ls,/usr/bin/tee,
/usr/bin/ed,/usr/sbin/logins,/usr/sam/lbin/usermod.sam,
/usr/sbin/groupadd,/usr/sbin/groupdel,/usr/sbin/groupmod,
/usr/bin/cp,/usr/bin/mkdir,/usr/bin/rm,/usr/bin/kill,
/usr/bin/hostname,/usr/sbin/acct/fwtmp
```

The following commands are used by the connector but are not needed in the sudoers file. However, if the sudo user is used, the user needs execute permissions on these commands.

- `tr`
- `cut`
- `egrep`
- `awk`
- `head`
- `sort`
- `ps`
- `sed`

   d. Validate the format of the `/etc/sudoers` file. Issue the command:

```
visudo -c
```

If syntax is wrong the command prompts an error message, for example:

```
$ visudo -c
>>> sudoers file: syntax error, line 30 <<<
parse error in /etc/sudoers near line 30
```

**Note:** The sudo access command paths that are listed here are an example. The actual command paths vary depending upon the resource. Ensure that the correct path is specified in the sudoers file.
3. Set the password for the newly created user. Issue the command:

bash-2.05b$ passwd tdiuser

**Command setup for sudo**

Some commands need sudo access.

The following table lists the files that are used by the commands. In this table:

- **Homedirectory** is a user specified directory. For example, `/home/username`.
- Shell can be `/bin/csh`, `/bin/sh`, and others.
- **Profilepath** can be `/homedirectory/.profile` depending on the shell that is defined by the user.

*Table 28. Sudo access command and file setup*

<table>
<thead>
<tr>
<th>Command</th>
<th>Files that are used by the command</th>
<th>Operation</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>cat</td>
<td><code>/var/adm/cron/at.allow</code></td>
<td>useradd</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td><code>/var/adm/cron/at.deny</code></td>
<td>usermod</td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td><code>/var/adm/cron/cron.allow</code></td>
<td>userdel</td>
<td>Solaris</td>
</tr>
<tr>
<td></td>
<td><code>/var/adm/cron/cron.deny</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>/etc/passwd</code></td>
<td>usermod</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td>userdel</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>set home directory</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>/etc/passwd</code></td>
<td>set umask</td>
<td>Linux - NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux - Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td></td>
<td><code>/etc/passwd</code></td>
<td>reconciliation</td>
<td>Linux - NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux - Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td></td>
<td><code>/etc/passwd</code></td>
<td>set home directory</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td>permissions</td>
<td>Linux - NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td><code>/etc/passwd</code></td>
<td>suspend and restore</td>
<td>Linux - NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td>account and userdel</td>
<td></td>
</tr>
</tbody>
</table>

Appendix C. Super user creation on a supported operating system
<table>
<thead>
<tr>
<th>Command</th>
<th>Files that are used by the command</th>
<th>Operation</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>/etc/passwd</td>
<td>set password and userdel</td>
<td>HP-UX-Trusted</td>
<td></td>
</tr>
<tr>
<td>/etc/passwd</td>
<td>usernmod</td>
<td>Linux - NonShadow, Linux - Shadow, HP-UX-Trusted, HP-UX-Nontrusted, Solaris</td>
<td></td>
</tr>
<tr>
<td>/etc/passwd</td>
<td>suspend and restore account and userdel</td>
<td>Linux - Shadow</td>
<td></td>
</tr>
<tr>
<td>/tcb/files/auth/usernamefolder/username</td>
<td>identify the operating system and the type of account (password or nopassword accounts)</td>
<td>HP-UX-Trusted</td>
<td></td>
</tr>
<tr>
<td>/tcb/files/auth/a/admin</td>
<td>profilepath</td>
<td>reconciliation</td>
<td></td>
</tr>
<tr>
<td>/tcb/files/auth/a/admin</td>
<td></td>
<td>Linux - NonShadow, Linux - Shadow, HP-UX-Trusted, HP-UX-Nontrusted, Solaris</td>
<td></td>
</tr>
<tr>
<td>/etc/at.allow</td>
<td>useradd</td>
<td>Linux - NonShadow, Linux - Shadow</td>
<td></td>
</tr>
<tr>
<td>/etc/at.deny</td>
<td>usernmod</td>
<td>Linux - NonShadow, Linux - Shadow</td>
<td></td>
</tr>
<tr>
<td>/etc/cron.allow</td>
<td>userdel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/etc/cron.deny</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>chmod</td>
<td>/var/adm/cron/at.allow</td>
<td>set permissions</td>
<td>AIX, HP-UX-Trusted, HP-UX-Nontrusted, Solaris</td>
</tr>
<tr>
<td>chmod</td>
<td>/var/adm/cron/at.den\y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>chmod</td>
<td>/var/adm/cron/cron.allow</td>
<td></td>
<td></td>
</tr>
<tr>
<td>chmod</td>
<td>/var/adm/cron/cron.deny</td>
<td></td>
<td></td>
</tr>
<tr>
<td>chmod</td>
<td>AIXPConnRes.sh</td>
<td>set permissions</td>
<td>AIX</td>
</tr>
<tr>
<td>chmod</td>
<td>ViosAixPConnRes.sh</td>
<td></td>
<td></td>
</tr>
<tr>
<td>chmod</td>
<td>mkvios.sh</td>
<td></td>
<td></td>
</tr>
<tr>
<td>chmod</td>
<td>HPMTtrustPConnRes.sh</td>
<td>set permissions</td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td>chmod</td>
<td>HPTrustPConnRes.sh</td>
<td>set permissions</td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td>chmod</td>
<td>CryptPwd</td>
<td></td>
<td></td>
</tr>
<tr>
<td>chmod</td>
<td>LinuxPConnRes.sh</td>
<td>set permissions</td>
<td>Linux - NonShadow</td>
</tr>
<tr>
<td>chmod</td>
<td>LinuxShadowPConnRes.sh</td>
<td>set permissions</td>
<td>Linux - Shadow</td>
</tr>
</tbody>
</table>
Table 28. Sudo access command and file setup (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Files that are used by the command</th>
<th>Operation</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>SolarisPConnRes.sh</td>
<td></td>
<td>set permissions</td>
<td>Solaris</td>
</tr>
<tr>
<td>LastAccessDateReader</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>homedirectory</td>
<td>Location of temporary files on resource. The default location is /tmp.</td>
<td>set permissions</td>
<td>AIX</td>
</tr>
<tr>
<td>/etc/at.allow</td>
<td></td>
<td>useradd</td>
<td>Linux - NonShadow</td>
</tr>
<tr>
<td>/etc/at.deny</td>
<td></td>
<td>usermod</td>
<td>Linux - Shadow</td>
</tr>
<tr>
<td>/etc/cron.allow</td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td>/etc/cron.deny</td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td>chsec</td>
<td>/etc/security/lastlog</td>
<td>restore account</td>
<td>AIX</td>
</tr>
<tr>
<td>chuser</td>
<td>homedirectory and shell</td>
<td>usermod</td>
<td>AIX</td>
</tr>
<tr>
<td>cp</td>
<td>/etc/skel/local.cshrc, profilepath</td>
<td>set umask</td>
<td>Solaris</td>
</tr>
<tr>
<td></td>
<td>/etc/csh.cshrc, profilepath</td>
<td>set umask</td>
<td>Linux - NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux - Shadow</td>
</tr>
<tr>
<td>ed</td>
<td>profilepath</td>
<td>set umask</td>
<td>Linux - NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux - Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td>fwtmp</td>
<td>/var/adm/wtmp</td>
<td>reconciliation</td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td>/var/adm/wtmps</td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td>Command</td>
<td>Files that are used by the command</td>
<td>Operation</td>
<td>Operating System</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------</td>
<td>--------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>grep</td>
<td>/etc/at.allow /etc/at.deny /etc/cron.allow /etc/cron.deny</td>
<td>reconciliation</td>
<td>Linux - NonShadow Linux - Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>lastlog</td>
<td>/var/log/lastlog</td>
<td>reconciliation</td>
<td>Linux - NonShadow Linux - Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ls -la</td>
<td>/etc/SuSE-release /etc/redhat-release /etc/debian_version</td>
<td>identify operating system</td>
<td>Linux - NonShadow Linux - Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>/tcb/files/auth/system/default</td>
<td>identify operating system</td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td>/usr/ios/cli/ios.level</td>
<td>identify operating system</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>homedirectory</td>
<td>delete home directory</td>
<td>AIX</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>profilepath</td>
<td>set umask</td>
<td></td>
<td>Linux - NonShadow Linux - Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>/var/adm/cron/at.allow /var/adm/cron/at.deny /var/adm/cron/cron.allow /var/adm/cron/cron.deny</td>
<td>useradd usermod userdel</td>
<td>AIX HP-UX-Trusted HP-UX-Nontrusted Solaris</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>homedirectory</td>
<td>reconciliation</td>
<td>Linux - NonShadow Linux - Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Location of temporary files on</td>
<td>reconciliation</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td>resource. The default location</td>
<td></td>
<td>Linux - NonShadow Linux - Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris</td>
</tr>
<tr>
<td></td>
<td>is /tmp. For example,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>/tmp/AIXPConnRes.sh</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td>Files that are used by the command</td>
<td>Operation</td>
<td>Operating System</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------</td>
<td>-----------</td>
<td>------------------</td>
</tr>
<tr>
<td>mkdir</td>
<td>Location of temporary files on resource. The default location is /tmp.</td>
<td>useradd</td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td>usermod</td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>userdel</td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cat</td>
<td>Solaris</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux - NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux - Shadow</td>
</tr>
<tr>
<td>mkuser</td>
<td>homedirectory</td>
<td>add user with home directory</td>
<td>AIX</td>
</tr>
<tr>
<td>mv</td>
<td>homedirectory</td>
<td>move home directory</td>
<td>AIX</td>
</tr>
<tr>
<td>rm -rf</td>
<td>homedirectory</td>
<td>delete home directory</td>
<td>AIX</td>
</tr>
<tr>
<td>tee</td>
<td>profilepath</td>
<td>set umask</td>
<td>Linux - NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux - Shadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HP-UX-Nontrusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux - NonShadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux - Shadow</td>
</tr>
</tbody>
</table>

Table 28. Sudo access command and file setup (continued)
Table 28. Sudo access command and file setup (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Files that are used by the command</th>
<th>Operation</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>test</strong></td>
<td><code>/tcb/files/auth/usernamefolder/username</code></td>
<td>identify the operating system and the type of account (password or nopassword accounts)</td>
<td>HP-UX-Trusted</td>
</tr>
<tr>
<td><strong>useradd</strong></td>
<td><code>homedirectory</code></td>
<td>add user with home directory</td>
<td>Linux - NonShadow, Linux - Shadow, HP-UX-Trusted, HP-UX-Nontrusted, Solaris</td>
</tr>
<tr>
<td><strong>usermod</strong></td>
<td><code>homedirectory</code> and <code>shell</code></td>
<td><code>usermod</code></td>
<td>Linux - NonShadow, Linux - Shadow, HP-UX-Trusted, HP-UX-Nontrusted, Solaris</td>
</tr>
</tbody>
</table>
Appendix D. Key-based authentication for the UNIX and Linux Adapter

An alternative to password-based authentication is Identity/Pubkey authentication. This type of authentication eliminates the need for static passwords.

A password can be captured by a keystroke logger or witnessed as you type it. Instead of providing a password, you have a key pair on your disk that you use to authenticate.

The following sections describe a typical SSH connection between a server and a client. For this setup example, the workstation that runs the IBM Tivoli Directory Integrator server is the SSH client and the managed resource is the SSH server.

Enabling RSA key-based authentication on UNIX and Linux operating systems

You can use RSA key-based authentication as an alternative to simple password authentication.

About this task

Perform this task on the managed resource:

Procedure

1. Use the `ssh-keygen` tool to create a key pair.
   a. Log in as the administrator user defined on the IBM Security Identity Manager service form.
   b. Start the `ssh-keygen` tool. Issue the command:
      ```
      mydesktop$# ssh-keygen -t rsa
      ```
   c. At the following prompt, accept the default or enter the file path where you want to save the key pair and press Enter.
      ```
      Generating public/private dsa key pair.
      Enter the file in which to save the key (/home/root/.ssh/id_rsa):
      ```
   d. At the following prompt, accept the default or enter the passphrase and press Enter.
      ```
      Enter the passphrase (empty for no passphrase):
      ```
   e. At the following prompt, confirm your passphrase selection and press Enter.
      ```
      Enter the same passphrase again:
      ```
      This example is a sample of the system response:
      ```
      Your identification was saved in /home/root/.ssh/id_rsa.
      Your public key was saved in /home/root/.ssh/id_rsa.pub.
      The key fingerprint is this value:
      ```

   **Note:** Although the `ssh-keygen` tool accepts a blank passphrase, the passphrase is required on the IBM Security Identity Manager service form.

2. Validate that the keys were generated.
   a. Issue the commands:
mydesktop$ cd $HOME/.ssh

mydesktop$ ls -l

A sample system response is:
-rw------- 1 root root 883 Jan 21 11:52 id_rsa
-rw-r--r-- 1 root root 223 Jan 21 11:52 id_rsa.pub

b. Issue the command:

mydesktop$ cat id_rsa

A sample system response is:

-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,7F4CF1E209817BA0
GuIQh4EdIp2DY1Kfg83eHic1lnCG5VC9/dumHd7AqEnlo241frIo8zg087Gv+tk
cvKd/pPCGmyCzy/are0wz3t3LKYWY0u0N7i+8H2Kkh6LmaspD6T6x309HTCyosj
jtuR5c4HbcRtoYhMByHEql1Est1azzz1Ir075QjScUG0IK1MbTExq1xUGjo97s+V
ge0okM+jMjaJD9r1bMz4wjWCRc2EhfcVYTA+ZE1W3HT3PfrjC6Hn9RKKFa6koM
FP1n5Fq6qjzHa0cjzC+hOKJfnpFphuFvGMJjfb99v 줄77LHeN4VqeQ/VyvHy7pn
wp7Gb6EJB86i4sXWJpXUSVStfnyQTYVBdoS7ay2zr3g/o+Akhnp/d0nh/1SHHN9FgUuf/
+E07EMKsHK9qQOZ4f6X8sApuunS/7aY5HIVCyU/4GW4sDEw7xFA25zD41bvV56
K52eLgL9s75mW1p5P99l1EELpQ6cS2yPxwADhs75P7QQUOYGFtMeHa/tI
3g105Pos7ek2J57mazmx33ocyI6E/7EIZ9KLysp5SR6Nqplx8KCV20k2x3QSHBF54EeoQ2+
SuSpA9Hg18+agk8b/1g3tFevT01cCuKQgl2bhrmNG6251jKgw9Ks0AL3I00u1l
D69D1B0bl6653pHO9bA6E1q3/5dqNYW8elQ5eINUIHB9ep8p+qv9q5Fb3qPCB6
Dbq109pYhT1gGRB015eQs1t1h23d7y/YV/Cp2m4fi+uHtC61kPRonj2Xh
p6HAPAF02znW0z1mVNYHtbjZ1bwYf/T0kmY0ok1SuQ=
-----END RSA PRIVATE KEY-----

c. Issue the command

mydesktop$ cat id_rsa.pub

A sample system response is this message:

ssh-rsa AAB3NzaC1yc2EAAAAbAAAIAA9xkGJ+BDRxSQfVxXYUXa4bcopCG4HwO3TL05i
fezBQx0e9UnWm1Nf1Xx83SaM36l+T5C3kJvY2+8p1IAe367/vYc1DznFQP395YnAfEj
YEa4B146uq1u0m+M+s/z/b07f1WTRbU6DWhHUmmeoX8U3ptKFZrRpb/

3. Enable key-based authentication in the /etc/ssh directory on the SSH server, the managed resource.

a. Ensure that the following lines exist in the sshd_config file:

# Should we allow Identity (SSH version 1) authentication?
# RSAAuthentication yes

# Should we allow Pubkey (SSH version 2) authentication?
# PubkeyAuthentication yes

# Where do we look for authorized public keys?
# If it doesn't start with a slash, then it is
# relative to the user's home directory
AuthKeysFile .ssh/authorized_keys

b. Restart the SSH server.

4. Copy the rsa.pub file to the SSH server, the managed resource.

5. If you have an existing authorized_keys file, edit it to remove any no-pty restrictions

6. Add the public key to the authorized_keys file, from the /.ssh directory. Issue the command:

ssh-server$ cat ../id_rsa.pub >> authorized_keys
Note: This command concatenates the RSA Pubkey to the `authorized_keys` file. For example, `$HOME/.ssh/authorized_keys`. If this file does not exist, the command creates it.

7. Copy the `id_rsa` private key file to the client workstation and set its ownership value to 755.

Note:
- Complete these steps. When you log in to the server from the client computer, you are prompted for a passphrase for the key instead of a user password.
- If the installed `ssh` uses the AES-128-CBC cipher, RXA cannot fetch the private key from the file. RSA key-based authentication does not work. To support RSA key-based authentication, take one of the following actions:
  - Install an `ssh` that uses the DES-EDE3-CBC cipher.
  - Install the RXA 2.3.0.9 package in your environment. RXA 2.3.0.9 supports the AES-128-CBC cipher.
  
RXA 2.3.0.9 is included in the base release of Tivoli Directory Integrator version 7.1.1, and is also available in Tivoli Directory Integrator version 7.0 fix pack 8 and Tivoli Directory Integrator version 7.1 fix pack 7.

### Enabling DSA key-based authentication on UNIX and Linux operating systems

You can use DSA key-based authentication as an alternative to simple password authentication.

**About this task**

Perform this task on the managed resource.

**Procedure**

1. Use the `ssh-keygen` tool to create a key pair.
   a. Log in as the administrator user defined on the IBM Security Identity Manager service form.
   b. Start the `ssh-keygen` tool. Issue the command:
      ```bash
      [root@ps2372 root]# ssh-keygen -t dsa
      ```
   c. At the following prompt, accept the default or enter the file path where you want to save the key pair and press Enter.
      ```plaintext
      Generating public/private dsa key pair.
      Enter the file in which to save the key (/root/.ssh/id_dsa):
      ```
   d. At the following prompt, accept the default or enter the passphrase and press Enter.
      ```plaintext
      Enter the passphrase (empty for no passphrase): passphrase
      ```
   e. At the following prompt, confirm your passphrase selection and press Enter.
      ```plaintext
      Enter the same passphrase again: passphrase
      ```

   This is a sample of the system response:
   ```plaintext
   Your identification is saved in /root/.ssh/id_dsa.
   Your public key is saved in /root/.ssh/id_dsa.pub.
   The key fingerprint is this one:
   ```
2. Validate that the keys were generated.
   a. Issue the commands:
      ```
      [root@ps2372 root]# cd root/.ssh
      [root@ps2372 .ssh]# ls -l
      
      A sample system response is this message:
      -rwxr-xr-x 1 root root 736 Dec 20 14:33 id_dsa
      -rw-r--r-- 1 root root 618 Dec 20 14:33 id_dsa.pub
      ```
   b. Issue the command:
      ```
      [root@ps2372 .ssh]# cat id_dsa
      ```
      A sample system response is this message:
      ```
      -----BEGIN DSA PRIVATE KEY-----
      Proc-Type: 4,ENCRYPTED
      DEK-Info: DES-EDE3-CBC,32242D3525AEDC64
      ...snip...
      -----END DSA PRIVATE KEY-----
      ```
      c. Issue the command:
      ```
      [root@ps2372 .ssh]# cat id_dsa.pub
      ```
      A sample system response is this message:
      ```
      ssh-dsa
      AAAAB3NzaC1kc3MAAACBAIHozHi6CHwvGDt7uYeEmm4SToj2neOo5mPOZfbj5
      ...snip...
      root@ps2372.persistent.co.in
      ```

3. Enable key-based authentication in the /etc/ssh directory on the SSH server, the managed resource.
   a. Ensure that the following lines exist in the sshd_config file:
      ```
      # Should we allow Identity (SSH version 1) authentication?
      DSAAuthentication yes
      # Should we allow Pubkey (SSH version 2) authentication?
      PubkeyAuthentication yes
      # Where do we look for authorized public keys?
      AuthorizedKeysFile .ssh/authorized_keys
      ```
   b. Restart the SSH server.
   c. Copy the dsa.pub file to the SSH server, the managed resource.
5. If you have an existing authorized_keys file, edit it to remove any **no-pty** restrictions.

6. Add the public key to the authorized_keys file, from the ./ssh directory. Issue the command:

   ```
   [root@ps2372 .ssh]# cat id_dsa.pub >> authorized_keys
   ```

   **Note:** This command concatenates the DSA Pubkey to the authorized_keys file. For example, $HOME/.ssh/authorized_keys. If this file does not exist, the command creates it.

7. Copy the id_dsa private key file to the client workstation and set its ownership value to 755.

   **Note:**
   - Complete these steps. When you log in to the server from the client computer, you are prompted for a passphrase for the key instead of a user password.
   - If the installed ssh uses the AES-128-CBC cipher, RXA cannot fetch the private key from the file. DSA key-based authentication does not work. To support DSA key-based authentication, take one of the following actions:
     - Install an ssh that uses the DES-EDE3-CBC cipher.
     - Install the RXA 2.3.0.9 package in your environment. RXA 2.3.0.9 supports the AES-128-CBC cipher.
     RXA 2.3.0.9 is included in the base release of Tivoli Directory Integrator version 7.1.1, and is also available in Tivoli Directory Integrator version 7.0 fix pack 8 and Tivoli Directory Integrator version 7.1 fix pack 7.

---

### Enabling RSA key-based authentication on UNIX and Linux operating systems with Tectia SSH

You can enable RSA key-based authentication on UNIX and Linux operating systems with Tectia SSH.

#### About this task

These instructions assume that the client user is allowed to log in to the remote host, where the Tectia Server is running, and using password authentication. Ensure that public-key authentication is enabled (the default) in the ssh-broker-config.xml and ssh-server-config.xml file. For example:

```
<authentication-methods>
  <auth-publickey />
  ...
</authentication-methods>
```

#### Procedure

- **Keys generated on an OpenSSH client:**
  1. Use the ssh-keygen tool to create a key pair.
     a. Log in as the administrator user defined on the IBM Security Identity Manager service form.
     b. Start the ssh-keygen tool. Type:
        ```
        mydesktop$ ssh-keygen -t rsa
        ```
c. At the prompt to generate a public/private RSA key pair, accept the default or enter the file path where you want to save the key pair and press Enter. For example:

   Generating public/private rsa key pair.
   Enter the file in which to save the key (/home/root/.ssh/id_rsa):

   d. At the prompt to enter a passphrase, accept the default or enter the passphrase and press Enter. For example:

   Enter passphrase (empty for no passphrase):

   e. Confirm your passphrase selection and press Enter. For example:

   Enter same passphrase again: passphrase

   The system response is similar to this example:

   Your identification has been saved in /home/root/.ssh/id_rsa.
   Your public key has been saved in /home/root/.ssh/id_rsa.pub.
   The key fingerprint is:

   Note: Although the ssh-keygen tool accepts a blank passphrase, the passphrase is required on the IBM Security Identity Manager service form.

2. Validate that the keys were generated.

   a. Enter these commands:

   mydesktop$ cd $HOME/.ssh
   mydesktop$ ls -l

   An example system response is:

   -rw------- 1 root root 883 Jan 21 11:52 id_rsa
   -rw-r--r-- 1 root root 223 Jan 21 11:52 id_rsa.pub

   b. Enter this command:

   mydesktop$ cat id_rsa

   An example system response is:

   -----BEGIN RSA PRIVATE KEY-----
   Proc-Type: 4,ENCRYPTED
   DEK-Info: DES-EDE3-CBC,7F4CF1E209817BA0
   Gu1Qh4EdipZDV11Kf9b38hcI1nCGsVC9/dunHd7AqEYlo241fRu1o8goB7Gv+tk
   cvKd/pPChkmyCzy/areFwz13KLWuyon7/1+H2XkhsBmpla/p01xH9VHFcyo3su
   J1v1R5c3WbcRt0YMB9j5QI54E1951azzl15rr7Qj35CUG1X5MbdDeQxIqUX6j19t5+y
   gE0kmQO+JmaJD91riMrzQj1wRTEJfJfCITYA7=21fNH3T3FrjCnhn0R0WFeA6km
   fPIjNgdVzCA0mCz+HOKJfKpFbhuFgM9Jf99VjZdZZ7LHeN4VqeQ/YyP97pn
   wp7Gbeb8961X8WuUpXUvolYNT8YVDsIayZt3g/o/AKh/dgk1SHHNFgUUF/+
   +EDEXMeTk1 sogar2zwT4t8p4unP5/7ag5MV1cU5/1WGW4sDEW7xfB2s2D41bvK5
   k52eWghm79m1npkP901eeLpgp0Sc2yPwx+AdFh5F7WPQBUFGfeMnha/
   tlgi105pxoe2I57mazmx33c0f1x6/7IZKs5spSTR6npq1x8Kcv20r2x3QSH8F54EoQ+2
   5udSpA0Hg18+aBChb/1g3teqY01cCtUkQQ52ubhbrNG25i1yKgo9Ks8AL700u1
   D69018r6y83HqLlyg6g3E1q3/5dQyWb5eL05e111Hq9ep8+quvHyF3qP9cBw
   D9+q109pXhTrGDB015eQ5t1j7th2gsY2yyYV/Cp2m4f1+wHiTcG51kPR0nD27Xh
   p6HApafO2wZ0l1nWYyHbJ1lbbwYf/0KmYuQk1SuQ=
   -----END RSA PRIVATE KEY-----

   c. Enter this command:

   mydesktop$ cat id_rsa.pub

   An example system response is:

   ssh-rsaAAB3NzaC1yc2EAAAIEAgj+BDLrXsQfVxXYxUx41c9copC4HwD3LTo5i
   fezBq0xeU9UnWFl4xan59yMdd6L+TfCkJVz+Ypl4we367/vhcn1DznFRP3975nATefj
   Ye4w1Elu7qtu0wm+4s/z/bf7fllWv1RrbiEDWHHHUmneoX8Bp/ptKFZaRpb/
   y7Eh6En= root@ps0701

3. After the key is generated, convert the public key for use on the Tectia SSH server.
a. On the local-host that is running openSSH, convert the openSSH public key to an SSH2 (tectia) public key by using `ssh-keygen`.

   ```
   [local-host]$ ssh-keygen -e -f ~/.ssh/id_rsa.pub > ~/.ssh/id_rsa_ssh2.pub
   ```

b. Install the public-key on the remote-host that is running SSH2.

   Create a new public key file on remote-host. Copy and paste the converted SSH2 key from local-host.

   ```
   [remote-host]$ vi ~/.ssh2/hostkey.pub
   ```

   For example:

   ```
   ---- BEGIN SSH2 PUBLIC KEY ----
   Comment: "1024-bit RSA, converted from OpenSSH by root@tivsun12.persistent.co.in"
   AAAAB3NzaC1yc2EAAAABJQAAAIAKZ8JgTeLjzOp49eIFcOdJLp5Gwv6mmrOQ+36C6oVcbs7X
   ---- END SSH2 PUBLIC KEY ----
   ```

c. Add the public key file name to the authorization file on the remote-host.

   For example:

   ```
   [remote-host]$ vi ~/.ssh2/authorization
   Key hostkey.pub
   ```

d. Copy the private key file (id_rsa) to the client workstation and set its ownership value to 600. Rename the private key file to hostkey on the client workstation.

   ```
   Keys generated on a Tectia SSH client: You can generate a key on the Tectia SSH client on a workstation with a UNIX or Linux operating system.
   ```

   1. Use the ssh-keygen-g3 tool to create a key pair.

      a. Start the `ssh-keygen` tool with this command:

         ```
         [root@vmw009053116054]:# ssh-keygen-g3 -t rsa
         ```

         The system response is similar to this example:

         ```
         Generating 2048-bit rsa key pair
         3 o.oOo.oOo.oO
         Key generated.
         2048-bit rsa, root@vmw009053116054, Tue Feb 25 2014 21:49:43 -0600
         ```

      b. At the prompt, accept the default or enter the file path where you want to save the passphrase and press `Enter`.

      c. At the next prompt, confirm the file path where you want to save the passphrase and press `Enter`.

         The system response is similar to this example:

         ```
         Private key saved to //.ssh2/id_rsa_2048_a
         Public key saved to //.ssh2/id_rsa_2048_a.pub
         ```

   2. Convert the private key created on the Tectia client. If the Tectia private key is passphrase protected, you must remove the first passphrase by using Tectia `keygen`. Press `Enter` when prompted for the new passphrase. For example:

      ```
      $ ssh-keygen-g3 -e id_rsa_2048_a
      ```

      a. At the prompt, provide the old passphrase. For example:

      ```
      Passphrase needed for key "id_rsa_2048_a".
      Passphrase: passphrase
      ```

      b. At the next prompt, type `yes` and press `Enter`. For example:

      ```
      Do you want to edit the key "" (yes or no)? yes
      ```

      c. At the next prompt, type `no` and press `Enter`. For example:
Your key comment is "id_rsa_2048_a ".
Do you want to edit it (yes or no)? no

d. At the next prompt, type yes and press Enter. For example:
   Do you want to edit the passphrase (yes or no)? yes

e. At the next prompt, press Enter. For example:
   New passphrase: passphrase

f. At the next prompt, press Enter. For example:
   Again: passphrase

g. At the next prompt, type no and press Enter. For example:
   Do you want to continue editing the key "" (yes or no)? no

h. At the next prompt, type yes and press Enter. For example:
   Do you want to save the key "" to file id_rsa_2048_a (yes or no)? yes

3. Use the OpenSSH keygen import.
   a. Type:
      ssh-keygen -i -f id_rsa_2048_a > my_openssh_privatekey
   b. Encrypt the key again with a passphrase using OpenSSH keygen. For example:
      ssh-keygen -p -f my_openssh_privatekey
   c. At the next prompt, accept the default or enter the passphrase and press Enter. For example:
      Enter new passphrase (empty for no passphrase): passphrase
   d. At the next prompt, confirm your passphrase selection and press Enter. For example:
      Enter same passphrase again: passphrase
   e. Rename the private key file my_openssh_privatekey to id_rsa_2048_a.
   f. Set the ownership value of this file to 600.

4. Install the public-key on the remote-host that is running Tectia SSH.
   a. Create a new public key file on remote-host. Copy and paste the id_rsa_2048_a.pub. For example:
      [remote-host]$ vi ~/.ssh2/id_rsa_2048_a.pub
      An example file is:
      ---- BEGIN SSH2 PUBLIC KEY ----
      Subject: root
      Comment: "2048-bit rsa, root@vmw009053116054, Tue Feb 25 2014 21:49:43 -0600"
      AAAAB3NzaC1yc2EAAAADAQABAAABAQDMy7Q3Z0pxlYCiA9wdJPgRuBR7NQvXIICIUXFbwx
      uJ66xkCnJc++JkZ1G+6tRItty+T8dxQE/98czGK6dgc9bbHV1Lvxn5v9aSFZMBaNy8T+p
      C1Pv/8L/kb6oXkgv4amqIQ9JnQhmwajKdNnW5w5RzDxv/fj0L1LdHUSWnEhPINdouEU/EE
      DzJhn2jRRmWx1h3XDege/n0UgdsAJkDaqj1Jld9HEk1Ph25eengp6y2YkJ9HqzVNdJLSYz
      NO/Bg5Nzran63y6CrS4q9Y9CioAkgfj9JS5/tpvPazLjoeMP8fzELp9swJ4vFMAuLpx9H
      jwXK/4a4Ngv7EyaektoqP
      ---- END SSH2 PUBLIC KEY ----
   b. Add the public key file name to the authorization file on the remote-host. For example:
      [remote-host]$ vi ~/.ssh2/authorization
      Key id_rsa_2048_a.pub

---

**Enabling DSA key-based authentication on UNIX and Linux operating systems with Tectia SSH**

You can enable DSA key-based authentication on UNIX and Linux operating systems with Tectia SSH.
About this task

These instructions assume that the client user is allowed to log in to the remote host, where the Tectia Server is running, and using password authentication. Ensure that public-key authentication is enabled (the default) in the ssh-broker-config.xml and ssh-server-config.xml file. For example:

```xml
<authentication-methods>
  <auth-publickey />
...
</authentication-methods>
```

Key-based authentication can be done using keys generated on an OpenSSH client or Tectia SSH client.

Procedure

- **Keys generated on an OpenSSH client:**
  1. Use the `ssh-keygen` tool to create a key pair.
     a. Log in as the administrator user defined on the IBM Security Identity Manager service form.
     b. Start the `ssh-keygen` tool. Type:
        ```
        mydesktop$ ssh-keygen -t dsa
        ```
     c. At the prompt to generate a public/private DSA key pair, accept the default or enter the file path where you want to save the key pair and press Enter. For example:
        ```
        Generating public/private dsa key pair.
        Enter the file in which to save the key (/home/root/.ssh/id_dsa):
        ```
     d. At the prompt to enter a passphrase, accept the default or enter the passphrase and press Enter. For example:
        ```
        Enter the passphrase (empty for no passphrase): passphrase
        ```
     e. Confirm your passphrase selection and press Enter. For example:
        ```
        Enter same passphrase again: passphrase
        ```
        The system response is similar to this example:
        ```
        Your identification has been saved in /home/root/.ssh/id_dsa.
        Your public key has been saved in /home/root/.ssh/id_dsa.pub.
        The key fingerprint is:
        root@ps2372.persistent.co.in
        ```
        **Note:** Although the `ssh-keygen` tool accepts a blank passphrase, the passphrase is required on the IBM Security Identity Manager service form.
  2. Validate that the keys were generated.
     a. Enter these commands:
        ```
        mydesktop$ cd $HOME/.ssh
        mydesktop$ ls -l
        ```
        An example system response is:
        ```
        -rwx------ 1 root root 883 Jan 21 11:52 id_dsa
        -rwxr--r-- 1 root root 223 Jan 21 11:52 id_dsa.pub
        ```
     b. Enter this command:
        ```
        mydesktop$ cat id_dsa
        ```
        An example system response is:
-----BEGIN DSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,32242D3525AEDC64
0M20m/BCLFNs+uj1cnQR3q01b5Swru1jbWvB/kvyTMIHqAxlANqgV1gFBG7xF0
vdffnQKnnjLcH8CGcuelYnmx4vS9fK91abN9WdK70tJzeTcHkahXbY7oX1t
Lnh3Qa2329agqr70xqcG1hOqebalGpeF9WhVqBE03cx+/L/5sQfpx0eG30nr0j1
+c1mXgmzUu2qsPL2cpxR90tqRdU40qWYDBele9YwUXTAGbe9wXG0iCm91F04WlWtWd24
Q7991w6UJReHKQq+vdrN7PgK32NNMmdoQdazKV2FL4TslgVgWofImpG65o0
FSc4GXrskR70QX1xapkhSRpJ3p6W1P4Nt4R/RC5mpW/yZr4qtZccw+AY60NA
QEVtJQen69LJnucyy9YfK2F7hmiCty7/onM1006d/aI116U40xh6qkasLGchi1TP
/Nfr1TQho491c1t9Hm54Bmeq9W9lS4a5xL1MmxvGcircju2XJl1mCmUqX9Hmhx
RI41aAta26TtxsBxShh/TVx34DvRJD4MSJLaNp3jnvAdYTM7Yis8Bu1TDfr8Zf6P9
Fa7VvFP4TyCfJUNW==
-----END DSA PRIVATE KEY-----

3. After the key is generated, convert the public key for use on the Tectia SSH server.
   a. On the local-host that is running openSSH, convert the openSSH public key to an SSH2 (tectia) public key by using **ssh-keygen**.

   ```
   [local-host]$ ssh-keygen -e -f ~/.ssh/id_dsa.pub > ~/.ssh/id_dsa_ssh2.pub
   ```

   b. Install the public-key on the remote-host that is running SSH2.

   Create a new public key file on remote-host. Copy and paste the converted SSH2 key from local-host.

   ```
   [remote-host]$ vi ~/.ssh2/hostkey.pub
   ```

   For example:

   ```
   BEGIN SSH2 PUBLIC KEY
   Comment: "1024-bit DSA, converted from OpenSSH
   by root@tivsun12.persistent.co.in"
   AAAAB3NzaC1kc3MAAAAIAK6H9Vi6ChwvG0t7ueYkEmm4STo2ne0o6mPOZfSpBjs
   KzzW8BuAx0xMgM0y3ZAIgmW1YQum4/uIh0xO0QDLJ3veFSXuX8bj580U1
   rC5SEQCYPQpub9hx3uzZnQnfIV04/NTc:jcpqQ0bdWsl0iyVtYVWyQVQmMjdf
   AAAAQ0boaDM/n07CyR+x46q5itYFAD/QAAAIvB6XZL/+/ChbyKgC62Cq6JRESQ
   12w1CPwCyvzwwfh4My0ye5Nk8sft1wY8Blus7XyCZCPbCNk0shsbFy9w
   /qXMbkrBTB+Qj06sebntxnwk/RrwmB9MS/kdMElgCounm9MMyJ105w5fG1
   PluYVh+yu9uTWPjyc8egAAIA1rKVY41r3fC17bCC5icwz6ekoC5Qs9016bMq
   1x14HJyTn70B6J35wyK68C215t01k66luXt/03d/GHAYa+5FcbJigLsnU0s
   R13Q63yKqOaP7TIKS7UYSOBFQw9q7jXHyshS8PvVUHK36h6YlLvhrX
   Jo7P6k6tQ== root@ps2372.persistent.co.in
   END SSH2 PUBLIC KEY
   ```

c. Add the public key file name to the authorization file on the remote-host.

   For example:

   ```
   [remote-host]$ vi ~/.ssh2/authorization
   Key hostkey.pub
   ```

d. Copy the private key file (id_dsa) to the client workstation and set its ownership value to 600. Rename the private key file to hostkey on the client workstation.

   **Keys generated on a Tectia SSH client:** You can generate a key on the Tectia SSH client on a workstation with a UNIX or Linux operating system.

1. Use the **ssh-keygen-g3** tool to create a key pair.

   a. Start the **ssh-keygen** tool with this command:

   ```
   [root@vmw00905316054]\# ssh-keygen-g3 -t dsa
   ```
The system response is similar to this example:

Generating 2048-bit dsa key pair
   92.o00...o00.o0
Key generated.
2048-bit dsa, root@vmw009053116054, Mon Mar 03 2014 01:57:28 -0600

b. At the prompt, accept the default or enter the file path where you want to save the passphrase and press Enter. For example:
   Passphrase : passphrase

c. At the prompt, confirm the file path where you want to save the passphrase and press Enter.
   The system response is similar to this example:
   Private key saved to //.ssh2/id_dsa_2048_a
   Public key saved to //.ssh2/id_dsa_2048_a.pub
   [root@vmw009053116054]:

2. Convert the private key created on the Tectia client. If the Tectia private key is passphrase protected, you must first remove the passphrase by using Tectia keygen. Press Enter when prompted for the new passphrase. For example:
   $ ssh-keygen-g3 -e id_dsa_2048_a
   a. At the prompt, provide the old passphrase. For example:
      Passphrase needed for the key " id_dsa_2048_a ".
      Passphrase: passphrase
   b. At the next prompt, type yes and press Enter. For example:
      Do you want to edit the key " " (yes or no)? yes
   c. At the next prompt, type no and press Enter. For example:
      Your key comment is " id_dsa_2048_a ".
      Do you want to edit it (yes or no)? no
   d. At the next prompt, type yes and press Enter. For example:
      Do you want to edit the passphrase (yes or no)? yes
   e. At the next prompt, press Enter. For example:
      New passphrase : passphrase
   f. At the next prompt, press Enter. For example:
      Again : passphrase
   g. At the next prompt, type no and press Enter. For example:
      Do you want to continue editing the key " " (yes or no)? no
   h. At the next prompt, type yes and press Enter. For example:
      Do you want to save the key " " to file id_dsa_2048_a (yes or no)? yes

3. Use the OpenSSH keygen import.
   a. Type:
      ssh-keygen -i -f id_dsa_2048_a > my_openssh_privatekey
   b. Encrypt the key again with a passphrase using OpenSSH keygen. For example:
      ssh-keygen -p -f my_openssh_privatekey
   c. At the next prompt, accept the default or enter the passphrase and press Enter. For example:
      Enter new passphrase (empty for no passphrase): passphrase
   d. At the next prompt, confirm your passphrase selection and press Enter. For example:
      Enter same passphrase again: passphrase
   e. Rename the private key file my_openssh_privatekey to id_dsa_2048_a.
f. Set the ownership value of this file to 600.

4. Install the public-key on the remote-host that is running Tectia SSH.

a. Create a new public key file on remote-host. Copy and paste the
   id_dsa_2048_a.pub. For example:
   [remote-host]$ vi ~/.ssh2/ id_dsa_2048_a.pub
   An example file is:
   ---- BEGIN SSH2 PUBLIC KEY ----
   Subject: root
   Comment: "2048-bit dsa, root@vmw009053116054,
   Mon Mar 03 2014 21:49:43\ -0600"
   AAAAB3NzaC1yc2EAAAAADAQABAAAAABADJy8CJ1A9wdJPGRuBR7NQVX11CIUXFbwx
   wJD6xqCnJc++JkZ1G+6tRlty+T8dXQE/98czG6dc9bbWq1Wxnx5v9aSfZMzA9y8T+p
   CIPV/0L/kbGoXkvg4amq1QkJnQhnaJKdNnWmWBMrcDkv/fj0L1LDhUSWnEhPinkoewU/EE
   DxrUhf2jRRHwXQihxDEge/n0Ugd5AkJaqtJ1dF9HEEkiPhZ25eeng0YmZk0JHQzVh0D2L5Yz
   WQ/Bg5Nzran63y6cR5t4oPY9C1oAkqj19J5P/tvPazLjoeMP8f+2ELp9suJ+VFPمولpq+x9H
   jwKX/4a4nWg7VeyaekoQp
   ---- END SSH2 PUBLIC KEY ----

b. Add the public key file name to the authorization file on the remote-host.
   For example:
   [remote-host]$ vi ~/.ssh2/authorization
   Key id_dsa_2048_a.pub
Appendix E. Definitions for ITDI_HOME and ISIM_HOME directories

ITDI_HOME is the directory where Tivoli Directory Integrator is installed. ISIM_HOME is the directory where IBM Security Identity Manager is installed.

ITDI_HOME
This directory contains the jars/connectors subdirectory that contains files for the adapters.

Windows
drive\Program Files\IBM\TDI\ITDI_VERSION

For example the path for version 7.1:
C:\Program Files\IBM\TDI\V7.1

UNIX
/opt/IBM/TDI/ITDI_VERSION

For example the path for version 7.1:
/opt/IBM/TDI/V7.1

ISIM_HOME
This directory is the base directory that contains the IBM Security Identity Manager code, configuration, and documentation.

Windows
path\IBM\isim

UNIX
path/IBM/isim
Appendix F. Support information

You have several options to obtain support for IBM products.

- “Searching knowledge bases”
- “Obtaining a product fix” on page 100
- “Contacting IBM Support” on page 100

Searching knowledge bases

You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods.

About this task

You can find useful information by searching the product documentation for IBM Security Identity Manager. However, sometimes you must look beyond the product documentation to answer your questions or resolve problems.

Procedure

To search knowledge bases for information that you need, use one or more of the following approaches:

1. Search for content by using the IBM Support Assistant (ISA).
   ISA is a no-charge software serviceability workbench that helps you answer questions and resolve problems with IBM software products. You can find instructions for downloading and installing ISA on the ISA website.

2. Find the content that you need by using the IBM Support Portal.
   The IBM Support Portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services. The IBM Support Portal lets you access the IBM electronic support portfolio from one place. You can tailor the pages to focus on the information and resources that you need for problem prevention and faster problem resolution. Familiarize yourself with the IBM Support Portal by viewing the demo videos (https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos) about this tool. These videos introduce you to the IBM Support Portal, explore troubleshooting and other resources, and demonstrate how you can tailor the page by moving, adding, and deleting portlets.

3. Search for content about IBM Security Identity Manager by using one of the following additional technical resources:
   - IBM Security Identity Manager version 6.0 technotes and APARs (problem reports)
   - IBM Security Identity Manager Support website
   - IBM Redbooks
   - IBM support communities (forums and newsgroups)

4. Search for content by using the IBM masthead search. You can use the IBM masthead search by typing your search string into the Search field at the top of any ibm.com page.

5. Search for content by using any external search engine, such as Google, Yahoo, or Bing. If you use an external search engine, your results are more likely to
include information that is outside the ibm.com domain. However, sometimes you can find useful problem-solving information about IBM products in newsgroups, forums, and blogs that are not on ibm.com.

**Tip:** Include “IBM” and the name of the product in your search if you are looking for information about an IBM product.

## Obtaining a product fix

A product fix might be available to resolve your problem.

### About this task

You can get fixes by following these steps:

### Procedure

1. Obtain the tools that are required to get the fix. You can obtain product fixes from the [Fix Central Site](http://www.ibm.com/support/fixcentral/).
2. Determine which fix you need.
3. Download the fix. Open the download document and follow the link in the “Download package” section.
4. Apply the fix. Follow the instructions in the “Installation Instructions” section of the download document.

## Contacting IBM Support

IBM Support assists you with product defects, answers FAQs, and helps users resolve problems with the product.

### Before you begin

After trying to find your answer or solution by using other self-help options such as technotes, you can contact IBM Support. Before contacting IBM Support, your company or organization must have an active IBM software subscription and support contract, and you must be authorized to submit problems to IBM. For information about the types of available support, see the [Support portfolio](http://www.ibm.com/software/support/isa/) topic in the “Software Support Handbook”.

### Procedure

To contact IBM Support about a problem:

1. Define the problem, gather background information, and determine the severity of the problem. For more information, see the [Getting IBM support](http://www.ibm.com/software/support/isa/) topic in the Software Support Handbook.
2. Gather diagnostic information.
3. Submit the problem to IBM Support in one of the following ways:
   - Using IBM Support Assistant (ISA):
     - Any data that has been collected can be attached to the service request. Using ISA in this way can expedite the analysis and reduce the time to resolution.
     b. Open ISA.
c. Click **Collection and Send Data**.
d. Click the **Service Requests** tab.
e. Click **Open a New Service Request**.
   • Online through the [IBM Support Portal](#): You can open, update, and view all of your service requests from the Service Request portlet on the Service Request page.
   • By telephone for critical, system down, or severity 1 issues: For the telephone number to call in your region, see the [Directory of worldwide contacts](#) web page.

**Results**

If the problem that you submit is for a software defect or for missing or inaccurate documentation, IBM Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM Support website daily, so that other users who experience the same problem can benefit from the same resolution.
Appendix G. Accessibility features for IBM Security Identity Manager

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

**Accessibility features**

The following list includes the major accessibility features in IBM Security Identity Manager.

- Support for the Freedom Scientific JAWS screen reader application
- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Keys that are discernible by touch but do not activate just by touching them
- Industry-standard devices for ports and connectors
- The attachment of alternative input and output devices

The IBM Security Identity Manager library, and its related publications, are accessible.

**Keyboard navigation**

This product uses standard Microsoft Windows navigation keys.

**Related accessibility information**

The following keyboard navigation and accessibility features are available in the form designer:

- You can use the tab keys and arrow keys to move between the user interface controls.
- You can use the Home, End, Page Up, and Page Down keys for more navigation.
- You can launch any applet, such as the form designer applet, in a separate window to enable the Alt+Tab keystroke to toggle between that applet and the web interface, and also to use more screen workspace. To launch the window, click **Launch as a separate window**.
- You can change the appearance of applets such as the form designer by using themes, which provide high contrast color schemes that help users with vision impairments to differentiate between controls.

**IBM and accessibility**

See the [IBM Human Ability and Accessibility Center](https://www.ibm.com/able) for more information about the commitment that IBM has to accessibility.
Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user’s responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbash-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.
IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM’s future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to
IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

If you are viewing this information softcopy, the photographs and color illustrations might not appear.

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

**Trademarks**

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at [http://www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Cell Broadband Engine and Cell/B.E. are trademarks of Sony Computer Entertainment, Inc., in the United States, other countries, or both and is used under license therefrom.
Privacy Policy Considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, and to tailor interactions with the end user or for other purposes. In many cases, no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

Index

A
accessibility x, 103
account
changing 67
creating 67
deleting 67
for adapters 13
last access attribute, Solaris 35
no password 36
password management 38
restoring 68
suspending 67
account form
attributes 57
descriptions 57
home directory permissions 30, 31
permissions 57
adapter ix
attributes 57
attributes, by actions 66
configuration 23
customization steps 23
feature customization 28
features 1
installation 9
  verifying 39
installation worksheet 8
maximum connection count 27
overview 1
reinstalling 55
script locations 32
silent installation 21
silent uninstallation 22
SSH remote connection 13
supported configurations 2
uninstallation 53
user accounts, creating 13
user management automation 1
adapter attributes
restoring accounts 38, 68
suspend accounts 67
adapter installation
Dispatcher requirement 9
troubleshooting errors 41
verifying 10
warnings 41
adapter profile
customization 23
importing 11, 51
objects that reference 53
operating system differences 23
password management 38
removal 53
upgrading 11, 51
verifying 12
adapters
upgrade 51
administration tasks, as super user 73
AIX operating systems
creating a user 73
super user 73
attributes
adapter, by action 66
erPosixHomeDir 30, 31
erPosixReconScriptLocation 33
for the adapter 57
for the group form
permissions 66
supported operating systems 66
password prompt 29
permissions, group form 66
authentication
DSA key pairs 87, 93
key-based 85
OpenSSH options 85
RSA key pairs 85, 89
B
BASE DIRECTORY 28
C
character support, non-English locales 32
commands
AIX operating systems, creating a user 73
for setting up sudo 79
HP-UX NonTrusted operating systems, creating a user 76
HP-UX Trusted operating systems, creating a user 78
Linux operating systems, creating a user 74
Solaris operating systems, creating a user 75
configuration
adapter 23
multiple servers 2
single server 2
supported 2
connectivity between server, resource ix
connector
installation 71
upgrades 51
creating
DSA key pairs 87, 93
home directory 28
RSA key pairs 85, 89
services 14
custom scripts, reconciling 33
customization
adapter features 28
adapter profile 23
password prompt attribute 29
D
default setting, silent mode 21
deleted user, ending user processes 34
directory integrator, uninstalling the adapter 53
dispatcher 1
  installation 9
upgrade 51
download, software 8
DSA key pairs, creating 87, 93
E
education x
ending user processes 34
erPosixDelUserInUse 34
erPosixHomeDir attribute 30, 31
erPosixReconScriptLocation 33
error messages 43
F
features
adapter 1
optional 29
G
group
add request 69
change request 69
delete request 71
primary 49
group form attributes 66
groupset, secondary 49
H
home directory
creating 28
permissions 30, 31
permissions, sudo user 48
umask value, sudo user 48
HP-UX NonTrusted operating systems
creating a user 76
super user 76
HP-UX Trusted operating systems
creating a user 78
super user 78
I
IBM
Software Support x
Support Assistant x
IBM Support Assistant 100
importing adapter profile 51
installation
adapter 9
adapter profile 11
connector 71
Dispatcher requirement 9
neutral
suspended user, ending active sessions 34
suspending accounts, attributes for 67
System Login Add request 67
System Login Change request 67
System Login Delete request 67
System Login Restore request 68
System Login Suspend request 67

terminology ix

test connection to managed resource 68
Tivoli Directory Integrator connector 1
trace.log file 11
training x
troubleshooting
  contacting support 100
  default shell 46
  getting fixes 100
  identifying problems 41
  log file searches 46
  messages 43
  reconciliation 46
  searching knowledge bases 99
  ssh issues 46
  sudo issues 46
  support website x
  techniques 41

uninstalling
  adapter from the directory integrator 53
  in silent mode 22
  steps 53
upgrading
  adapter profile 23, 51
  adapters 51
  connector 51
  dispatcher 51
user account
  previously suspended 68
  restoring 68
user management automation, adapter 1
user session, ending after suspension 34
user-defined scripts 26

verification
  dispatcher installation 9
  installation 39
  operating system prerequisites 6
  operating system requirements 6
  software prerequisites 6
  software requirements 6
  vi command 28

warning messages 43